

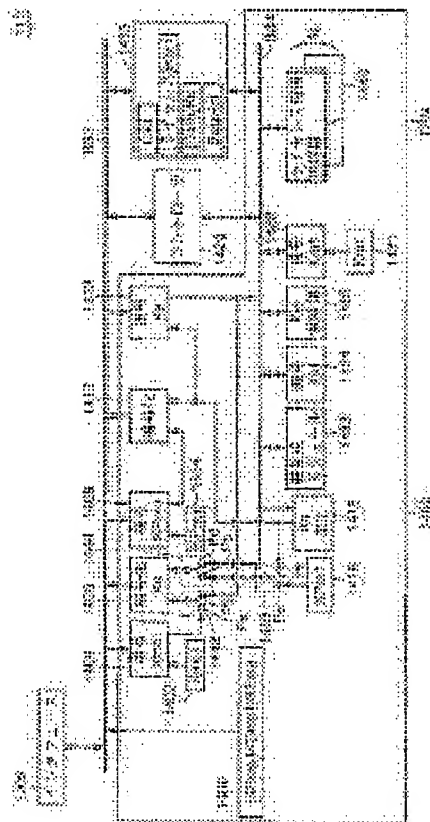
DATA RECORDING APPARATUS, AND DATA REPRODUCING DEVICE**Publication number:** JP2002026890 (A)**Publication date:** 2002-01-25**Inventor(s):** HIOKI TOSHIAKI; KANAMORI YOSHIKAZU; HORI YOSHIHIRO**Applicant(s):** SANYO ELECTRIC CO**Classification:**

- international: **G06F21/20; G06F15/00; H04L9/08; H04L9/32; H04N7/167; H04Q7/38; G06F21/20; G06F15/00; H04L9/08; H04L9/32; H04N7/167; H04Q7/38; (IPC1-7): H04L9/08; G06F15/00; H04L9/32; H04N7/167; H04Q7/38**

- European:

Application number: JP20000202032 20000704**Priority number(s):** JP20000202032 20000704**Abstract of JP 2002026890 (A)**

PROBLEM TO BE SOLVED: To provide a data recording apparatus and a data reproducing device that can protect encrypted contents data by excluding external intrusions and to provide a terminal employing them. **SOLUTION:** A memory card 110 is provided with a key generating module 1432, an encryption section 1434 and a memory 1415. The key generating module 1432 generates a couple of a private encryption key and a public decoding key on the basis of information received from a portable telephone set onto which the memory card 110 is loaded. The memory 1415 stores the private encryption key and the open decoding key is transmitted to the data reproducing device and stored therein. In the case of reproducing encrypted contents data, the encryption section 1434 transmits a contents key encrypted by the private encryption key to the portable telephone set on the basis of the private encryption key read from the memory 1415 and the contents key.



Data supplied from the **esp@cenet** database — Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-26890

(P2002-26890A)

(43)公開日 平成14年1月25日(2002.1.25)

(51)Int.Cl. ⁷	識別記号	F I	フォーマット(参考)
H 0 4 L 9/08		G 0 6 F 15/00	3 3 0 G 5 B 0 8 5
G 0 6 F 15/00	3 3 0	H 0 4 L 9/00	6 0 1 A 5 C 0 6 4
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 S 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 0 1 E 5 K 0 6 7
H 0 4 N 7/167			6 7 5 D

審査請求 未請求 請求項の数18 O L (全 29 頁) 最終頁に続く

(21)出願番号 特願2000-202032(P2000-202032)

(22)出願日 平成12年7月4日(2000.7.4)

(71)出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(72)発明者 日置 敏昭

大阪府守口市京阪本通2丁目5番5号 三
洋電機株式会社内

(72)発明者 金森 美和

大阪府守口市京阪本通2丁目5番5号 三
洋電機株式会社内

(74)代理人 100064746

弁理士 深見 久郎 (外3名)

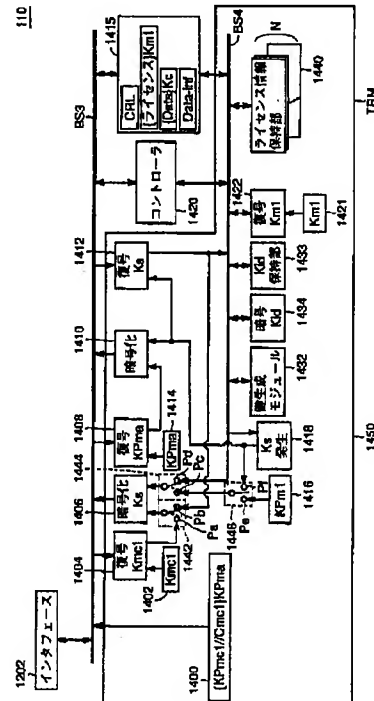
最終頁に続く

(54)【発明の名称】 データ記録装置、およびデータ再生装置

(57)【要約】

【課題】 暗号化されたコンテンツデータを外部からの進入を排除して保護できるデータ記録装置、データ再生装置、およびそれを用いた端末装置を提供する。

【解決手段】 メモリカード1110は、鍵生成モジュール1432と、暗号部1434と、メモリ1415とを備える。鍵生成モジュール1432は、メモリカード1110が装着された携帯電話機から入力された情報に基づいて一対の秘密暗号鍵と公開復号鍵とを生成する。秘密暗号鍵はメモリ1415に記録され、公開復号鍵はデータ再生装置へ送付されて保持される。暗号化コンテンツデータの再生時、暗号部1434は、メモリ1415から読出された秘密暗号鍵とコンテンツ鍵とに基づいて、秘密暗号鍵によって暗号化されたコンテンツ鍵を携帯電話機へ送信する。



【特許請求の範囲】

【請求項 1】 バスと、

前記バスに接続され、外部とデータのやり取りを行なう
インタフェース部と、

前記バスに接続された制御部と、

前記バスに接続され、ユーザからの指示に従って外部から
入力される情報に基づいて暗号鍵と、前記暗号鍵によ
って暗号化されたデータを復号する復号鍵とを生成する
鍵生成モジュールと、

前記バスに接続され、前記暗号鍵を保持する鍵保持部
と、

前記バスに接続され、前記鍵保持部に保持された前記暗
号鍵によって暗号化を行なう暗号部と、

前記バスに接続され、外部から入力されたデータを記録
するメモリとを備え、

前記制御部は、前記鍵生成モジュールによって生成され
た前記暗号鍵を前記鍵保持部に記録し、前記復号鍵を前
記インタフェース部を介して外部へ出力する、データ記
録装置。

【請求項 2】 ユーザからの出力要求により、

前記制御部は、前記メモリから前記データを取得して前
記暗号部に与え、前記暗号部において前記鍵保持部に保
持された暗号鍵によって暗号化されたデータを前記イン
タフェース部を介して外部へ出力する、請求項 1 に記載
のデータ記録装置。

【請求項 3】 前記データの入力時、

前記制御部は、前記暗号部において前記暗号鍵によって
暗号化されたデータを前記メモリに記録する、請求項 1
に記載のデータ記録装置。

【請求項 4】 ユーザからの出力要求により、

前記制御部は、前記メモリから前記暗号鍵によって暗号
化された前記データを読み出して前記インタフェース部を
介して外部へ出力する、請求項 3 に記載のデータ記録装
置。

【請求項 5】 前記制御部は、前記データの出力先を認
証する認証手段を有し、前記認証手段によって前記出力
先が認証されたときに、前記データを出力する、請求項
1 から請求項 4 のいずれか 1 項に記載のデータ記録装
置。

【請求項 6】 データを暗号化した暗号化データと、前
記暗号化データを復号して前記データを得るための復号
鍵であるライセンスキーとを記録するデータ記録装置で
あって、

バスと、

前記バスに接続され、外部とやり取りを行なうインタ
フェース部と、

前記バスに接続された制御部と、

前記バスに接続され、ユーザからの指示に従って外部から
入力される情報に基づいて暗号鍵と、前記暗号鍵によ
って暗号化されたデータを復号する復号鍵とを生成する

鍵生成モジュールと、

前記バスに接続され、前記暗号鍵を保持する鍵保持部
と、

前記バスに接続され、前記鍵保持部に保持された前記暗
号鍵によって暗号化を行なう暗号部と、

前記バスに接続され、外部から入力された前記ライセン
スキーおよび暗号化データを記録するメモリとを備え、
前記制御部は、前記鍵生成モジュールによって生成され
た前記暗号鍵を前記鍵保持部に記録し、前記復号鍵を前
記インタフェース部を介して外部へ出力する、データ記
録装置。

【請求項 7】 ユーザからの出力要求により、

前記制御部は、前記メモリから前記ライセンスキーを取
得して前記暗号部に与え、前記暗号部において前記鍵保
持部に保持された暗号鍵によって暗号化されたライセン
スキーと前記メモリから取得した前記暗号化データとを
前記インタフェース部を介して外部へ出力する、請求項
6 に記載のデータ記録装置。

【請求項 8】 前記インタフェース部を介してライセン
スキーが入力されたとき、

前記制御部は、前記暗号部において前記暗号鍵によって
暗号化されたライセンスキーを前記メモリに記録する、
請求項 6 に記載のデータ記録装置。

【請求項 9】 ユーザからの出力要求により、

前記制御部は、前記メモリから前記暗号化データと、前
記暗号鍵によって暗号化されたライセンスキーとを読み出
して前記インタフェース部を介して外部へ出力する、請
求項 8 に記載のデータ記録装置。

【請求項 10】 前記制御部は、前記ライセンスキーの

出力先を認証する認証手段を有し、前記認証手段により
前記出力先が認証されたときに、前記ライセンスキーを
出力する、請求項 6 から請求項 9 のいずれか 1 項に記載
のデータ記録装置。

【請求項 11】 前記暗号鍵は、前記復号鍵と非対称で
ある、請求項 1 または請求項 6 に記載のデータ記録装
置。

【請求項 12】 データを記録し、外部からの入力によ
って一对の暗号鍵と復号鍵とを生成し、前記暗号鍵によ
って暗号化された前記データと、前記復号鍵とを外部へ
出力するデータ記録装置から前記データを再生するデー
タ再生装置であって、

バスと、

前記バスに接続され、ユーザが情報を入力する入力部
と、

前記バスに接続された制御部と、

前記バスに接続され、前記データ記録装置とデータのや
り取りを行なうインタフェース部と、

前記バスに接続され、前記データ記録装置において生成
された復号鍵を保持する鍵メモリと、

前記バスに接続され、前記データ記録装置から入力され

3

た前記暗号鍵によって暗号化されたデータを、前記鍵メモリからの前記復号鍵によって復号する復号部とを含み、

前記制御部は、ユーザによって前記入力部から入力された情報を前記インタフェース部を介して前記データ記録装置へ出力し、前記データ記録装置が前記情報に基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、データ再生装置。

【請求項 13】 データを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、前記暗号鍵によって暗号化された前記データと、前記復号鍵とを外部へ出力するデータ記録装置から前記データを再生するデータ再生装置であって、

バスと、

前記バスに接続され、ユーザが指示を入力する入力部と、

前記バスに接続された制御部と、

前記バスに接続され、前記データ記録装置とデータのやり取りを行なうインタフェース部と、

前記バスに接続され、前記データ記録装置において生成された復号鍵を保持する鍵メモリと、

前記バスに接続され、前記データ記録装置から入力された前記暗号鍵によって暗号化されたデータを、前記鍵メモリからの前記復号鍵によって復号する復号部とを含み、

前記制御部は、機器 ID を保持し、前記入力部からのユーザの指示によって前記機器 ID を前記インタフェース部を介して前記データ記録装置へ出力し、前記データ記録装置が前記機器 ID に基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、データ再生装置。

【請求項 14】 前記制御部は、データ供給装置から携帯電話または簡易携帯電話網を介して受信したデータを前記メモリに記録するとともに、電話番号を保持し、前記入力部からのユーザの指示によって前記電話番号を前記インタフェース部を介して前記データ記録装置へ出力し、前記データ記録装置が前記電話番号に基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、請求項 13 に記載のデータ再生装置。

【請求項 15】 データを暗号化した暗号化データと、前記暗号化データを復号して前記データを得るための復号鍵であるライセンスキーとを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、前記暗号鍵によって暗号化された前記ライセンスキーと、前記復号鍵とを外部へ出力するデータ記録装置から前記データを再生するデータ再生装置であって、

バスと、

4

前記バスに接続され、ユーザが情報を入力する入力部と、

前記バスに接続された制御部と、

前記バスに接続され、前記データ記録装置とデータのやり取りを行なうインタフェース部と、

前記バスに接続され、前記データ記録装置において生成された復号鍵を保持する鍵メモリと、

前記バスに接続され、前記データ記録装置から入力された前記暗号鍵によって暗号化されたライセンスキーを、前記鍵メモリからの前記復号鍵によって復号する第 1 の復号部と、

前記バスに接続され、前記データ記録装置から入力された前記暗号化データを、前記第 1 の復号部において復号されたライセンスキーによって復号する第 2 の復号部と、

前記第 2 の復号部において復号されたデータを再生する再生部とを含み、

前記制御部は、ユーザによって前記入力部から入力された情報を前記インタフェース部を介して前記データ記録装置へ出力し、前記データ記録装置が前記情報に基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、データ再生装置。

【請求項 16】 データを暗号化した暗号化データと、前記暗号化データを復号して前記データを得るための復号鍵であるライセンスキーとを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、前記暗号鍵によって暗号化された前記ライセンスキーと、前記復号鍵とを外部へ出力するデータ記録装置から前記データを再生するデータ再生装置であって、

バスと、

前記バスに接続され、ユーザが指示を入力する入力部と、

前記バスに接続された制御部と、

前記バスに接続され、前記データ記録装置とデータのやり取りを行なうインタフェース部と、

前記バスに接続され、前記データ記録装置において生成された復号鍵を保持する鍵メモリと、

前記バスに接続され、前記データ記録装置から入力された前記暗号鍵によって暗号化されたライセンスキーを、前記鍵メモリからの前記復号鍵によって復号する第 1 の復号部と、

前記バスに接続され、前記データ記録装置から入力された前記暗号化データを、前記第 1 の復号部において復号されたライセンスキーによって復号する第 2 の復号部と、

前記第 2 の復号部において復号されたデータを再生する再生部とを含み、

前記制御部は、機器 ID を保持し、前記入力部からのユーザの指示によって前記機器 ID を前記インタフェース

部を介して前記データ記録装置へ出力し、前記データ記録装置が前記機器IDに基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、データ再生装置。

【請求項17】 前記制御部は、データ供給装置から携帯電話または簡易携帯電話網を介して受信したデータを前記メモリに記録するとともに、電話番号を保持し、前記入力部からのユーザの指示によって前記電話番号を前記インタフェース部を介して前記データ記録装置へ出力し、前記データ記録装置が前記電話番号に基づいて生成した一対の暗号鍵と復号鍵のうち、前記復号鍵を前記インタフェース部を介して取得して前記鍵メモリに入力する、請求項16に記載のデータ再生装置。

【請求項18】 前記暗号鍵は、前記復号鍵と非対称である、請求項12から請求項17のいずれか1項に記載のデータ再生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムによって配信されたコンテンツデータを外部からの進入を排除して保護できるデータ記録装置およびデータ再生装置に関するものである。

【0002】

【従来の技術】 近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】 このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】 したがって、このような情報通信網上において音楽データや画像データ等の著作権者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】 一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】 ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽デー

タのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【0007】 しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】 このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】 この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【0010】 そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンスキーを送信する。そして、暗号化コンテンツデータやライセンスキーを配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】 最終的に、配信サーバは、メモリカード個々に固有の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータとをメモリカードに送信する。そして、メモリカードは、受信したライセンスキーと暗号化コンテンツデータをメモリカードに記録する。

【0012】 メモリカードは、公開暗号鍵と非対称な秘密復号鍵を保持しており、この秘密復号鍵は、公開暗号鍵で暗号化されたデータを復号できる鍵である。メモリカードは、その秘密復号鍵を携帯電話機へ送信し、携帯電話機は暗号化されたライセンスキーを、受信した秘密復号鍵で復号し、暗号化コンテンツデータを復号したラ

イセンスキーによって復号してコンテンツデータを再生する。

【0013】上記のようなデータ配信システムにおいては、配信サーバは、ライセンスキーの配信に対して課金し、暗号化した状態でライセンスキーや暗号化コンテンツデータをメモリカードへ送信するので、著作権は十分に保護されている。また、暗号化コンテンツデータを受信した携帯電話機のユーザがその暗号化コンテンツデータを他人にコピーしても、その他人は暗号化コンテンツデータを復号するライセンスキーを取得できないので、そのままでは暗号化コンテンツデータを再生できない。他人が暗号化コンテンツデータを再生するには、配信サーバへアクセスし、別途、料金を支払ってライセンスキーを購入する必要がある。したがって、受信した暗号化コンテンツデータを他人がコピーすることは自由であるが、その他人は、新たにライセンスキーを購入しなければならないので、自由なコピーを許容しながら著作権をも保護している。

【0014】

【発明が解決しようとする課題】しかし、暗号化コンテンツデータを再生するためにメモリカードと携帯電話機との間でデータのやり取りを行なう場合、メモリカードで発生させた共通鍵と携帯電話機で発生させた共通鍵とによって暗号化を行なっている。したがって、メモリカードおよび携帯電話機に固有の鍵を用いてデータのやり取りを行なうことができず、外部からの進入に対して十分な保護がなされていなかった。

【0015】そこで、本発明はかかる問題を解決するためになされたものであり、その目的は、暗号化されたコンテンツデータを外部からの進入を排除して保護できるデータ記録装置、およびデータ再生装置を提供することである。

【0016】

【課題を解決するための手段および発明の効果】この発明によるデータ記録装置は、バスと、バスに接続され、外部とデータのやり取りを行なうインタフェース部と、バスに接続された制御部と、バスに接続され、ユーザからの指示に従って外部から入力される情報に基づいて暗号鍵と、暗号鍵によって暗号化されたデータを復号する復号鍵とを生成する鍵生成モジュールと、バスに接続され、暗号鍵を保持する鍵保持部と、バスに接続され、鍵保持部に保持された暗号鍵によって暗号化を行なう暗号部と、バスに接続され、外部から入力されたデータを記録するメモリとを備え、制御部は、鍵生成モジュールによって生成された暗号鍵を鍵保持部に記録し、復号鍵を前インタフェース部を介して外部へ出力する。

【0017】この発明によるデータ記録装置においては、データ記録装置の一例であるメモリカードが装着された携帯電話機からユーザによって情報が入力される。そうすると、メモリカードの制御部は携帯電話機から情

報を入力して鍵生成モジュールに入力する。そうすると、鍵生成モジュールは、入力された情報に基づいて暗号鍵と復号鍵とを生成する。そして、生成された暗号鍵は鍵保持部に保持され、復号鍵はインタフェース部を介して外部へ出力される。

【0018】したがって、この発明によれば、データ記録装置は、装着された端末装置から入力された情報に基づいて暗号鍵と復号鍵とを生成できる。その結果、外部からの進入を防止してデータ記録装置と端末装置とのデータのやり取りを行なうことができる。

【0019】好ましくは、ユーザからの出力要求により、制御部は、メモリからデータを取得して暗号部に与え、暗号部において鍵保持部に保持された暗号鍵によって暗号化されたデータをインタフェース部を介して外部へ出力する。

【0020】データ記録装置が装着された端末装置を介してユーザから出力要求があったとき、制御部はメモリからデータを取得して暗号部へ入力する。そして、暗号部は暗号鍵によってデータを暗号化する。制御部は暗号鍵によって暗号化されたデータを外部へ出力する。そうすると、データ再生装置は、暗号鍵によって暗号化されたデータを復号鍵によって復号して再生する。

【0021】したがって、この発明によれば、データ記録装置が装着された端末装置から入力された情報に基づいて生成された暗号鍵と復号鍵とを用いてデータを端末装置へ送信して再生できる。その結果、データの再生過程に外部から進入できず、データを十分に保護できる。

【0022】好ましくは、データの入力時、制御部は、暗号部において暗号鍵によって暗号化されたデータをメモリに記録する。

【0023】データが入力されるとき、暗号部は、鍵保持部から読出された暗号鍵によってデータを暗号化する。そして、制御部は、暗号鍵によって暗号化されたデータをメモリに記録する。

【0024】したがって、この発明によれば、データ記録装置に記録されたデータを再生するとき、データに外部から容易にアクセスできず、データを十分に保護できる。

【0025】好ましくは、ユーザからの出力要求により、制御部は、メモリから暗号鍵によって暗号化されたデータを読出してインタフェース部を介して外部へ出力する。

【0026】ユーザから出力要求があると、制御部はメモリに記録された暗号化データを読出してデータ再生装置へ出力する。そして、データ再生装置において、暗号化データは復号鍵によって復号されて再生される。

【0027】したがって、この発明によれば、暗号化データの再生時、暗号化データをメモリから読出してデータ再生装置へ送信すれば良く、迅速な再生動作を実現できる。

【0028】好ましくは、データ記録装置の制御部は、データの出力先を認証する認証手段を有し、認証手段によって出力先が認証されたときに、データを出力する。

【0029】データ記録装置に記録されたデータを再生するとき、データの出力先が正規の出力先であることが確認されてから、その出力先へデータが出力される。

【0030】したがって、この発明によれば、正規な出力先へのみデータを出力でき、データ記録装置に記録されたデータに対する十分な保護が可能である。

【0031】また、この発明によるデータ記録装置は、データを暗号化した暗号化データと、暗号化データを復号してデータを得るための復号鍵であるライセンスキーとを記録するデータ記録装置であって、バスと、バスに接続され、外部とやり取りを行なうインタフェース部と、バスに接続された制御部と、バスに接続され、ユーザからの指示に従って外部から入力される情報に基づいて暗号鍵と、暗号鍵によって暗号化されたデータを復号する復号鍵とを生成する鍵生成モジュールと、バスに接続され、暗号鍵を保持する鍵保持部と、バスに接続され、鍵保持部に保持された暗号鍵によって暗号化を行なう暗号部と、バスに接続され、外部から入力されたライセンスキーおよび暗号化データを記録するメモリとを備え、制御部は、鍵生成モジュールによって生成された暗号鍵を鍵保持部に記録し、復号鍵をインタフェース部を介して外部へ出力する。

【0032】この発明によるデータ記録装置においては、データ記録装置の一例であるメモリカードが装着された携帯電話機からユーザの指示によって情報が入力される。そうすると、メモリカードの制御部は携帯電話機から情報を入力して鍵生成モジュールに入力する。そうすると、鍵生成モジュールは、入力された情報に基づいて暗号鍵と復号鍵とを生成する。そして、生成された暗号鍵は鍵保持部に保持され、復号鍵はインタフェース部を介して外部へ出力される。また、メモリには暗号化データと、その暗号化データを復号するためのライセンスキーとが記録される。

【0033】したがって、この発明によれば、データ記録装置は、装着された端末装置から入力された情報に基づいて暗号鍵と復号鍵とを生成できる。その結果、外部からの進入を防止してデータ記録装置と端末装置との暗号化データのやり取りを行なうことができる。

【0034】好ましくは、ユーザからの出力要求により、制御部は、メモリからライセンスキーを取得して暗号部に与え、暗号部において鍵保持部に保持された暗号鍵によって暗号化されたライセンスキーとメモリから取得した暗号化データとをインタフェース部を介して外部へ出力する。

【0035】データ記録装置が装着された端末装置を介してユーザから出力要求があったとき、制御部はメモリからライセンスキーを取得して暗号部へ入力する。そし

て、暗号部は暗号鍵によってライセンスキーを暗号化する。制御部は暗号鍵によって暗号化されたライセンスキーを外部へ出力する。そうすると、データ再生装置は、暗号鍵によって暗号化されたライセンスキーを復号鍵によって復号し、その復号されたライセンスキーを用いて暗号化データを復号して再生する。

【0036】したがって、この発明によれば、データ記録装置が装着された端末装置から入力された情報に基づいて生成された暗号鍵と復号鍵とを用いてライセンスキーを暗号化し、その暗号化されたライセンスキーを端末装置へ送信して再生できる。その結果、暗号化データの再生過程に外部から進入できず、データを十分に保護できる。

【0037】好ましくは、インタフェース部を介してライセンスキーが入力されたとき、制御部は、暗号部において暗号鍵によって暗号化されたライセンスキーをメモリに記録する。

【0038】ライセンスキーが入力される時、暗号部は、鍵保持部から読出された暗号鍵によってデータを暗号化する。そして、制御部は、暗号鍵によって暗号化されたライセンスキーをメモリに記録する。

【0039】したがって、この発明によれば、外部から入力されたライセンスキーに対してデータ記録装置において生成された暗号鍵を用いて暗号化を行なうことができる。その結果、暗号化データの再生過程で用いるライセンスキーを、外部からの進入を防止してデータ再生装置へ送信することができ、暗号化データの十分な保護が可能である。

【0040】好ましくは、ユーザからの出力要求により、制御部は、メモリから暗号化データと、暗号鍵によって暗号化されたライセンスキーとを讀出してインタフェース部を介して外部へ出力する。

【0041】ユーザから出力要求があると、制御部はメモリに記録された暗号化データと、データ記録装置において生成された暗号鍵によって暗号化されたライセンスキーとを讀出して外部へ出力する。そして、たとえば、データ再生装置において、暗号化されたライセンスキーは復号鍵によって復号され、その復号されたライセンスキーによって暗号化データが復号されてデータが再生される。

【0042】したがって、この発明によれば、暗号化データの再生時、暗号化されたライセンスキーと、暗号化データとをメモリから讀出してデータ再生装置へ送信すれば良く、迅速な再生動作を実現できる。

【0043】好ましくは、データ記録装置の制御部は、ライセンスキーの出力先を認証する認証手段を有し、認証手段により出力先が認証されたときに、ライセンスキーを出力する。

【0044】データ記録装置に記録された暗号化データを再生するとき、暗号化データの出力先が正規の出力先

であることが確認されてから、その出力先へ暗号化データが出力される。

【0045】したがって、この発明によれば、正規な出力先へのみ暗号化データを出力でき、データ記録装置に記録された暗号化データに対する十分な保護が可能である。

【0046】好ましくは、暗号鍵は、復号鍵と非対称である。データ記録装置は、入力された情報に基づいて非対称な暗号鍵と復号鍵とを生成する。

【0047】したがって、暗号鍵を秘密鍵として、また復号鍵を公開鍵として取り扱うことができる。その結果、復号鍵だけを再生装置へ送信して保持し、再生時に暗号鍵によって暗号化されたデータを再生装置へ送信すればよく、データを十分に保護できる。

【0048】また、この発明によるデータ再生装置は、データを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、暗号鍵によって暗号化されたデータと、復号鍵とを外部へ出力するデータ記録装置からデータを再生するデータ再生装置であって、バスと、バスに接続され、ユーザが情報を入力する入力部と、バスに接続された制御部と、バスに接続され、データ記録装置とデータのやり取りを行なうインタフェース部と、バスに接続され、データ記録装置において生成された復号鍵を保持する鍵メモリと、バスに接続され、データ記録装置から入力された暗号鍵によって暗号化されたデータを、鍵メモリからの復号鍵によって復号する復号部とを含み、制御部は、ユーザによって入力部から入力された情報をインタフェース部を介してデータ記録装置へ出力し、データ記録装置が情報に基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵をインタフェース部を介して取得して鍵メモリに入力する。

【0049】この発明によるデータ再生装置においては、ユーザによって情報が入力されると、その入力された情報はデータ記録装置へ送信され、データ記録装置において情報に基づいて一対の暗号鍵と復号鍵とが生成される。そして、データ再生装置は、生成された復号鍵をデータ記録装置から受取り、鍵メモリに保持する。

【0050】したがって、この発明によれば、データ再生装置は、入力した情報に基づいて生成された復号鍵を保持できる。その結果、データの再生時、データ記録装置から暗号鍵によって暗号化されたデータのみを受け取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【0051】また、この発明によるデータ再生装置は、データを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、暗号鍵によって暗号化されたデータと、復号鍵とを外部へ出力するデータ記録装置からデータを再生するデータ再生装置であって、バスと、バスに接続され、ユーザが指示を入力する入力部と、バスに接続された制御部と、バスに接続され、データ記録装置

とデータのやり取りを行なうインタフェース部と、バスに接続され、データ記録装置において生成された復号鍵を保持する鍵メモリと、バスに接続され、データ記録装置から入力された暗号鍵によって暗号化されたデータを、鍵メモリからの復号鍵によって復号する復号部とを含み、制御部は、機器IDを保持し、入力部からのユーザの指示によって機器IDをインタフェース部を介してデータ記録装置へ出力し、データ記録装置が機器IDに基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵をインタフェース部を介して取得して鍵メモリに入力する。

【0052】この発明によるデータ再生装置においては、そのデータ再生装置の機器IDがデータ記録装置へ送信され、データ記録装置において機器IDに基づいて一対の暗号鍵と復号鍵とが生成される。そして、データ再生装置は、生成された復号鍵をデータ記録装置から受取り、鍵メモリに保持する。

【0053】したがって、この発明によれば、データ再生装置に固有の情報に基づいて一対の暗号鍵と復号鍵とを生成できる。

【0054】また、データ再生装置は、データの再生時、データ記録装置から暗号鍵によって暗号化されたデータのみを受け取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【0055】好ましくは、データ再生装置の制御部は、データ供給装置から携帯電話または簡易携帯電話網を介して受信したデータをメモリに記録するとともに、電話番号を保持し、入力部からのユーザの指示によって電話番号をインタフェース部を介してデータ記録装置へ出力し、データ記録装置が電話番号に基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵を前記インタフェース部を介して取得して鍵メモリに入力する。

【0056】データ再生装置の制御部は、ユーザからの指示によって保持している電話番号をデータ記録装置へ送信する。そうすると、データ記録装置は、送信された電話番号に基づいて一対の暗号鍵と復号鍵とを生成する。そして、データ再生装置は、生成された復号鍵をデータ記録装置から受取り、鍵メモリに保持する。

【0057】したがって、この発明によれば、データ再生装置に固有の情報に基づいて一対の暗号鍵と復号鍵とを生成できる。

【0058】また、この発明によれば、データ再生装置は、データの再生時、データ記録装置から暗号鍵によって暗号化されたデータのみを受け取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【0059】また、この発明によるデータ再生装置は、データを暗号化した暗号化データと、暗号化データを復号してデータを得るための復号鍵であるライセンスキー

とを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、暗号鍵によって暗号化されたライセンスキーと、復号鍵とを外部へ出力するデータ記録装置からデータを再生するデータ再生装置であって、バスと、バスに接続され、ユーザが情報を入力する入力部と、バスに接続された制御部と、バスに接続され、データ記録装置とデータのやり取りを行なうインタフェース部と、バスに接続され、データ記録装置において生成された復号鍵を保持する鍵メモリと、バスに接続され、データ記録装置から入力された暗号鍵によって暗号化されたライセンスキーを、鍵メモリからの復号鍵によって復号する第1の復号部と、バスに接続され、データ記録装置から入力された暗号化データを、第1の復号部において復号されたライセンスキーによって復号する第2の復号部と、第2の復号部において復号されたデータを再生する再生部とを含み、制御部は、ユーザによって入力部から入力された情報をインタフェース部を介してデータ記録装置へ出力し、データ記録装置が情報に基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵をインタフェース部を介して取得して鍵メモリに入力する。

【0060】この発明によるデータ再生装置は、入力された情報をデータ記録装置へ送信し、データ記録装置においてその送信した情報に基づいて生成された復号鍵をデータ記録装置から受取って鍵メモリに保持する。そして、暗号化データの再生時、データ再生装置は、暗号鍵によって暗号化されたライセンスキーと、暗号化データとをデータ記録装置から受取り、暗号化されたライセンスキーを復号鍵によって復号し、その復号したライセンスキーによって暗号化データを復号してデータを再生する。

【0061】したがって、この発明によれば、データ再生装置は、データの再生時、暗号化データと、暗号鍵によって暗号化されたライセンスキーとをデータ記録装置から受取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【0062】この発明によるデータ再生装置は、データを暗号化した暗号化データと、暗号化データを復号してデータを得るための復号鍵であるライセンスキーとを記録し、外部からの入力によって一対の暗号鍵と復号鍵とを生成し、暗号鍵によって暗号化されたライセンスキーと、復号鍵とを外部へ出力するデータ記録装置からデータを再生するデータ再生装置であって、バスと、バスに接続され、ユーザが指示を入力する入力部と、バスに接続された制御部と、バスに接続され、データ記録装置とデータのやり取りを行なうインタフェース部と、バスに接続され、データ記録装置において生成された復号鍵を保持する鍵メモリと、バスに接続され、データ記録装置から入力された暗号鍵によって暗号化されたライセンスキーを、鍵メモリからの復号鍵によって復号する第1の

復号部と、バスに接続され、データ記録装置から入力された暗号化データを、第1の復号部において復号されたライセンスキーによって復号する第2の復号部と、第2の復号部において復号されたデータを再生する再生部とを含み、制御部は、機器IDを保持し、入力部からのユーザの指示によって機器IDをインタフェース部を介してデータ記録装置へ出力し、データ記録装置が機器IDに基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵をインタフェース部を介して取得して鍵メモリに入力する。

【0063】この発明によるデータ再生装置は、保持する機器IDをデータ記録装置へ送信し、データ記録装置においてその送信した機器IDに基づいて生成された復号鍵をデータ記録装置から受取って鍵メモリに保持する。そして、暗号化データの再生時、データ再生装置は、暗号鍵によって暗号化されたライセンスキーと、暗号化データとをデータ記録装置から受取り、暗号化されたライセンスキーを復号鍵によって復号し、その復号したライセンスキーによって暗号化データを復号してデータを再生する。

【0064】したがって、この発明によれば、データ再生装置に固有の機器IDに基づいて暗号鍵と復号鍵とを生成できる。

【0065】また、この発明によれば、データ再生装置は、データの再生時、暗号化データと、暗号鍵によって暗号化されたライセンスキーとをデータ記録装置から受取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【0066】好ましくは、データ再生装置の制御部は、データ供給装置から携帯電話または簡易携帯電話網を介して受信したデータをメモリに記録するとともに、電話番号を保持し、入力部からのユーザの指示によって電話番号をインタフェース部を介してデータ記録装置へ出力し、データ記録装置が電話番号に基づいて生成した一対の暗号鍵と復号鍵のうち、復号鍵をインタフェース部を介して取得して鍵メモリに入力する。

【0067】この発明によるデータ再生装置は、保持する電話番号をデータ記録装置へ送信し、データ記録装置においてその送信した電話番号に基づいて生成された復号鍵をデータ記録装置から受取って鍵メモリに保持する。そして、暗号化データの再生時、データ再生装置は、暗号鍵によって暗号化されたライセンスキーと、暗号化データとをデータ記録装置から受取り、暗号化されたライセンスキーを復号鍵によって復号し、その復号したライセンスキーによって暗号化データを復号してデータを再生する。

【0068】したがって、この発明によれば、データ再生装置に固有の電話番号に基づいて暗号鍵と復号鍵とを生成できる。

【0069】また、この発明によれば、データ再生装置

は、データの再生時、暗号化データと、暗号鍵によって暗号化されたライセンスキーとをデータ記録装置から受取ればよく、外部からの進入を防止してデータ記録装置との間でデータのやり取りを行なうことができる。

【0070】好ましくは、暗号鍵は、復号鍵と非対称である。データ記録装置は、入力された情報に基づいて非対称な暗号鍵と復号鍵とを生成する。

【0071】したがって、暗号鍵を秘密鍵として、また復号鍵を公開鍵として取り扱うことができる。その結果、復号鍵だけを再生装置へ送信して保持し、再生時に暗号鍵によって暗号化されたデータを再生装置へ送信すればよく、データを十分に保護できる。

【0072】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0073】図1は、本発明によるデータ再生装置が再生の対象とする暗号化コンテンツデータをデータ記録装置（メモリカード）へ配信するデータ配信システムの全体構成を概略的に説明するための概念図である。

【0074】なお、以下では携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画データ等を配信する場合においても、さらには、他の情報通信網を介して配信する場合においても適用することが可能なものである。

【0075】図1を参照して、著作権の存在する音楽データを管理するライセンスサーバ10は、データ配信を求めてアクセスしてきた携帯電話ユーザの携帯電話機に装着されたメモリカードが正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア20である携帯電話会社に、このような暗号化コンテンツデータを与える。

【0076】配信キャリア20は、自己の携帯電話網を通じて、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバ10に中継する。ライセンスサーバ10は、配信リクエストがあると、認証サーバ12によりメモリカード等が正規の機器であることを確認し、要求されたコンテンツデータをさらに暗号化した上で配信キャリア20の携帯電話網を介して、各携帯電話ユーザの携帯電話機を介して接続されたメモリカードに対してコンテンツデータを配信する。

【0077】図1においては、たとえば携帯電話ユーザの携帯電話機100には、着脱可能なメモリカード110が装着される構成となっている。メモリカード110

は、携帯電話機100により受信された暗号化コンテンツデータを受取って、上記配信にあたって行なわれた暗号化については復号した上で、携帯電話機100中の音楽再生部（図示せず）に与える。

【0078】さらに、たとえば携帯電話ユーザは、携帯電話機100に接続したヘッドホン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0079】以下では、このようなライセンスサーバ10と配信キャリア20と併せて、配信サーバ30と総称することにする。

【0080】また、このような配信サーバ30から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0081】このような構成とすることで、まず、メモリカード110を利用しないと、配信サーバ30からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【0082】しかも、配信キャリア20において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア20が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0083】しかも、このようなコンテンツデータの配信は、携帯電話機網というクローズなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【0084】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話ユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号化鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0085】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびコンテンツ再生回路（携帯電話機）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0086】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0087】まず、配信サーバ30より配信されるデータについて説明する。Dataは、音楽データ等のコンテンツデータである。コンテンツデータDataには、ライセンスキーKcで復号可能な暗号化が施される。ライセンスキーKcによって復号可能な暗号化が施された暗号化コンテンツデータ{Data}Kcがこの形式で配信サーバ30より携帯電話ユーザに配布される。

【0088】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0089】さらに、配信サーバ30からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Data-infが配布される。また、ライセンス情報としては、コンテンツデータDataを識別するためのコードであるコンテンツIDおよびライセンスの発行を特定できる管理コードであるライセンスIDや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1および再生回路における制御情報である再生回路制御情報AC2等が存在する。以後、ライセンスキーKcとコンテンツIDとライセンスIDとアクセス制御情報AC1と再生回路制御情報AC2とを併せて、ライセンスと総称することとする。

【0090】図3は、図1に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【0091】本発明の実施の形態においては、記録装置(メモリカード)やコンテンツ再生回路(携帯電話機)のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストCRL(Class Revocation List)の運用を行なう。以下では、必要に応じて記号CRLによって禁止クラスリスト内のデータを表わすこともある。

【0092】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止されるコンテンツ再生回路およびメモリカードのクラスをリストアップした禁止クラスリストデータCRLが含まれる。

【0093】禁止クラスリストデータCRLは、配信サーバ30内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には変更点のみを反映した差分データCRL_datの配信サーバ30側より発生して、これに応じてメモリカード内の禁止クラスリストCRLが書替えられる構成とする。また、禁止クラスリストのバージョンについては、CRL_verをメモリカード側より出力し、これを配信サーバ30側

で確認することによってバージョン管理を実行する。差分データCRL_datには新たなバージョンの情報も含まれる。また、バージョン情報として、更新日時を用いることも可能である。

【0094】このように、禁止クラスリストCRLを、配信サーバのみならずメモリカード内においても保持運用することによって、クラス固有すなわちコンテンツ再生回路およびメモリカードの種類に固有の復号鍵の破られた、コンテンツ再生回路およびメモリカードへのライセンスキーの供給を禁止する。このため、コンテンツ再生回路ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【0095】このように、メモリカード内の禁止クラスリストCRLは配信時に逐次データを更新する構成とする。また、メモリ回路内における禁止クラスリストCRLの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール(Tamper Resistance Module)に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータCRLを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【0096】コンテンツ再生回路(携帯電話機)およびメモリカードには固有の公開暗号鍵Kp_pnおよびKp_mcmがそれぞれ設けられ、公開暗号鍵Kp_pnおよびKp_mcmはコンテンツ再生回路(携帯電話機)の固有の秘密復号鍵Kp_nおよびメモリカード固有の秘密復号鍵K_mcmによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【0097】また、再生回路およびメモリカードのクラス証明書として、CrtfnおよびCmcmがそれぞれ設けられる。これらのクラス証明書は、メモリカードおよびコンテンツ再生部(携帯電話機)のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が拾得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【0098】これらのメモリカードおよびコンテンツ再生部固有の公開暗号鍵およびクラス証明書は、認証データ{Kp_mcm/Cmcm}Kp_maの形式で、出荷時にメモリカードおよび携帯電話機にそれぞれ記録される。後ほど詳細に説明するが、Kp_maは配信システム全体で共通の公開認証鍵である。

【0099】図4は、図1に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【0100】メモ리카ード外とメモ리카ード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ30、携帯電話機100、メモ리카ード110において生成される共通鍵Ks1~Ks3が用いられる。

【0101】ここで、共通鍵Ks1~Ks3は、配信サーバ、携帯電話機もしくはメモ리카ード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ks1~Ks3を「セッションキー」とも呼ぶこととする。

【0102】これらのセッションキーKs1~Ks3は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモ리카ードによって管理される。具体的には、セッションキーKs1は、配信サーバによって配信セッションごとに発生される。セッションキーKs2は、メモ리카ードによって配信セッションごとに発生し、セッションキーKs3は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンスキー等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0103】また、メモ리카ード100内のデータ処理を管理するための鍵として、メモ리카ードという媒体ごとに設定される公開暗号鍵Kpmと、公開暗号鍵Kpmで暗号化されたデータを復号することが可能なメモ리카ードごとに固有の秘密復号鍵Kmが存在する。

【0104】さらに、携帯電話機のID、携帯電話機の電話番号、時刻等の携帯電話機から選ばれる情報に基づいて生成され、暗号化コンテンツデータの再生時にメモ리카ードと携帯電話機とのデータのやり取りに用いられる一対の公開暗号鍵Kpidと秘密復号鍵Kidが存在する。

【0105】図5は、図1に示したライセンスサーバ10の構成を示す概略ブロック図である。

【0106】ライセンスサーバ10は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスID等の配信情報を保持するための情報データベース304と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース302と、禁止クラスリストCRLを管理するCRLデータベース306と、情報データベース304、課金データベース302およびCRLデータベース306からのデータをデータバスBS1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0107】データ処理部310は、データバスBS1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御されて、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、メモ리카ードおよび携帯電話機から送られてきた認証のための復号することでその正当性が認証できる状態に暗号化した認証データ {Kpmcm/Cmcm} Kpmaを通信装置350およびデータバスBS1を介して受けて、公開認証鍵Kpmaによる復号処理を行なう復号処理部312と、セッションキー発生部316より生成されたセッションキーKs1を復号処理部312によって得られた公開暗号鍵Kpmcmを用いて暗号化して、データバスBS1に出力するための暗号化処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをデータバスBS1より受けて、復号処理を行なう復号処理部320を含む。

【0108】データ処理部310は、さらに、配信制御部315から与えられるライセンスキーKcおよび再生回路制御情報AC2を、復号処理部320によって得られたメモ리카ード固有の公開暗号鍵Kpmによって暗号化するための暗号化処理部326と、暗号化処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してデータバスBS1に出力するための暗号化処理部328を含む。

【0109】ライセンスサーバ10の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0110】図6は、図1に示した携帯電話機100の構成、すなわち、本発明の実施の形態によるデータ再生装置を含む携帯電話機の構成を説明するための概略ブロック図である。

【0111】携帯電話機100は、携帯電話網により無線伝送される信号を受信するためのアンテナ1102と、アンテナ1102からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ1102に与えるための送受信部1104と、携帯電話機100の各部のデータ授受を行なうためのデータバスBS2と、データバスBS2を介して携帯電話機100の動作を制御するためのコントローラ1106を含む。なお、コントローラ1106は、機器ID、電話番号等の携帯電話機100から得られる情報を保持する。

【0112】携帯電話機100は、さらに、外部からの指示を携帯電話機100に与えるための操作ボタン部1108と、コントローラ1106等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ1110と、通常の通話動作において、データバスBS2を介して与えられる受信データに基づいて音声再生するための音声再生部1112と、外部とのデ

ータのやり取りを行なう外部インタフェース部 1107 とを含む。

【0113】携帯電話機 100 は、さらに、配信サーバ 30 からのコンテンツデータ（音楽データ）を記憶しつつ復号化処理するための着脱可能なメモリカード 110 と、メモリカード 110 とデータバス BS2 との間のデータの授受を制御するためのメモリカードインタフェースと、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵 Kppl およびクラス証明書 Crtf1 を公開認証鍵 Kpma で復号することでその正当性が認証できる状態に暗号化した認証データ {Kppl / Crtf1} Kpma を保持する認証データ保持部 1500 を含む。

【0114】携帯電話機 100 は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵である Kp1、および Kp2 を保持する Kpx 保持部 1502 と、データバス BS2 から受けたデータを Kp1 または Kp2 によって復号しメモリカードによって発生されたセッションキー Ks2 を得る復号処理部 1504 と、メモリカード 110 に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード 110 との間でデータバス BS2 上においてやり取りされるデータを暗号化するためのセッションキー Ks3 を乱数等により発生するセッションキー発生部 1508 と、生成されたセッションキー Ks3 を復号処理部 1504 によって得られたセッションキー Ks2 によって暗号化しデータバス BS2 に出力する暗号処理部 1506 と、データバス BS2 上のデータをセッションキー Ks3 によって復号して出力する復号処理部 1510 とを含む。

【0115】携帯電話機 100 は、さらに、メモリカード 110 にて発生した対をなす秘密暗号鍵 Kid と公開復号鍵 Kpid のうちの 1 つである公開復号鍵 Kpid をメモリカード 110 から受けて保持する鍵メモリ 1512 と、復号処理部 1510 の出力である秘密暗号鍵 Kid にて暗号化されたライセンスキーおよび再生回路制御情報 {Kc / AC2} Kpid を鍵メモリ 1512 に保持された公開復号鍵 Kpid によって復号処理を行ない、復号したライセンスキー Kc を復号処理部 1516 へ、再生回路制御情報 AC2 をデータバス BS2 を介してコントローラ 1106 へ出力する復号処理部 1514 を含む。

【0116】携帯電話機 100 は、さらに、データバス BS2 より暗号化コンテンツデータ {Data} Kc を受けて、復号処理部 1510 より取得したライセンスキー Kc によって復号しコンテンツデータを出力する復号処理部 1516 と、復号処理部 1516 の出力を受けてコンテンツデータを再生するための音楽再生部 1518 と、音楽再生部 1518 の出力をディジタル信号からアナログ信号に変換する DA 変換器 1519 と、音声再生部 1112 の出力をディジタル信号からアナログ信号に

変換する DA 変換器 1113 と、DA 変換器 1113 と DA 変換器 1519 との出力を受けて、動作モードに応じて選択的に端子 1114 または端子 1520 から出力するためのスイッチ 1521 と、スイッチ 1521 の出力を受けて、データを増幅する増幅器 1522 と、増幅器 1522 の出力を受けてヘッドホン 130 と接続するための接続端子 1530 とを含む。

【0117】なお、図 6 においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【0118】また、携帯電話ユーザの利便性を図るために、携帯電話機 100 のうち、通話処理に関するブロックを除いた、図 6 において実線で囲まれる、コンテンツデータの配信および再生に関するブロック全体を音楽再生モジュール 1550 として、着脱可能なモジュール化する構成を採用することも可能である。

【0119】携帯電話機 100 の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0120】図 7 は、図 6 に示したメモリカード 110 の構成を説明するための概略ブロック図である。

【0121】既に説明したように、メモリカードの固有の公開暗号鍵および秘密復号鍵として、Kpmcm および Kmcm が設けられ、メモリカードのクラス証明書 Cmc が設けられるが、メモリカード 110 においては、これらは自然数 $m=1$ でそれぞれ表わされるものとする。

【0122】したがって、メモリカード 110 は、認証データ {Kpmc1 / Cmc1} Kpma を保持する認証データ保持部 1400 と、メモリカードの種類ごとに設定される固有の復号鍵である Km c1 を保持する Km c 保持部 1402 と、メモリカードごとに固有に設定される秘密復号鍵 Km1 を保持する Km1 保持部 1421 と、Km1 によって復号可能な公開暗号鍵 Kpm1 を保持する Kpm1 保持部 1416 とを含む。認証データ保持部 1400 は、メモリカードの種類およびクラスごとにそれぞれ設定される公開暗号鍵 Kpmc1 およびクラス証明書 Cmc1 を公開認証鍵 Kpma で復号することでその正当性が認証できる状態に暗号化した認証データ {Kpmc1 / Cmc1} Kpma として保持する。

【0123】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンスキーの管理をメモリカード単位で実行することが可能になる。

【0124】メモリカード 110 は、さらに、メモリカードインタフェースとの間で信号をインタフェース 12

02を介して授受するデータバスBS3と、データバスBS3にメモ리카ードインタフェースから与えられるデータから、メモ리카ードの種類ごとに固有の秘密復号鍵Kmc1をKmc1保持部1402から受けて、配信サーバ30が配信セッションにおいて生成したセッションキーKs1を接点Paに出力する復号処理部1404と、KPma保持部1414から公開認証鍵KPmaを受けて、データバスBS3に与えられるデータを公開認証鍵KPmaによる復号処理を実行して復号結果を暗号化処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1444によって選択的に与えられるデータを暗号化してデータバスBS3に出力する暗号化処理部1406を含む。

【0125】メモ리카ード110は、さらに、配信、および再生の各セッションにおいてセッションキーKs2を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーKs2を復号処理部1408によって得られる公開暗号鍵KPpnもしくはKPmcmによって暗号化してデータバスBS3に送出する暗号化処理部1410と、BS3よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号し、復号結果をデータバスBS4に送出する復号処理部1412を含む。

【0126】メモ리카ード110は、さらに、携帯電話機100のコントローラ1106が保持する機器ID、電話番号等の情報をインタフェース1202およびデータバスBS3を介して入力し、入力した情報に基づいて秘密暗号鍵Kidと、秘密暗号鍵Kidと対を成す公開復号鍵KPidとを生成する鍵生成モジュール1432と、秘密暗号鍵Kidを保持するKid保持部1433と、Kid保持部1433に保持された秘密暗号鍵Kidによって暗号処理を行なう暗号処理部1434を含む。

【0127】メモ리카ード110は、さらに、データバスBS4上のデータを公開暗号鍵KPm1と対をなすメモ리카ード110固有の秘密復号鍵Km1によって復号するための復号処理部1422と、公開暗号鍵KPm1で暗号化されている、ライセンスキーKc、再生回路制御情報AC2および再生情報(コンテンツID、ライセンスID、アクセス制御情報AC1)と、暗号化されていない禁止クラスリストのバージョン更新のための差分データCRL_d a tによって逐次更新される禁止クラスリストデータCRLとをデータバスBS4より受けて格納するとともに、暗号化コンテンツデータ{Data}Kcおよび付加情報Data_i n fをデータバスBS3より受けて格納するためのメモリ1415を含む。メモリ1415は、例えば半導体メモリによって構成される。

【0128】メモ리카ード110は、さらに、復号処理部1422によって得られるメモ리카ード110にて参照されるライセンスの一部、すなわち、ライセンスID、コンテンツIDおよびアクセス制限情報AC1を保持するためのライセンス情報保持部1440と、データバスBS3を介して外部との間でデータ授受を行ない、データバスBS4との間で再生情報等を受けて、メモ리카ード110の動作を制御するためのコントローラ1420を含む。

【0129】ライセンス情報保持部1440は、データバスBS4との間でライセンスID、データコンテンツIDデータおよびアクセス制限情報AC1のデータの授受が可能である。ライセンス情報保持部1440は、N個(N:自然数)のバンクを有し、各ライセンスに対応するライセンス情報をバンクごとに保持する。

【0130】なお、図7において、実線で囲んだ領域は、ライセンス保護モジュール1450を構成する。また、メモリ1415は、メモ리카ード110内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールTRMに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール(Tamper Resistance Module)である。

【0131】次に、図1に示すデータ配信システムの各セッションにおける動作についてフローチャートを参照して詳しく説明する。

【0132】図8および図9は、図1に示すデータ配信システムにおけるコンテンツの購入時に発生する配信動作(以下、配信セッションともいう)を説明するための第1および第2のフローチャートである。

【0133】図8および図9においては、携帯電話ユーザが、メモ리카ード110を用いることで、携帯電話機100を介して配信サーバ30から音楽データであるコンテンツデータの配信を受ける場合の動作を説明している。

【0134】まず、携帯電話ユーザの携帯電話機100から携帯電話ユーザにより操作ボタン部1108のキーボタンの操作等によって、配信リクエストがなされる(ステップS100)。

【0135】メモ리카ード110においては、この配信リクエストに応じて、認証データ保持部1400より認証データ{KPmc1//Cmc1}KPmaが出力される(ステップS102)。

【0136】携帯電話機100は、メモ리카ード110から受理した認証のための認証データ{KPmc1//Cmc1}KPmaに加えて、コンテンツID、ライセンス購入条件のデータACとを配信サーバ30に対して送信する(ステップS104)。

【0137】配信サーバ30では、携帯電話機100からコンテンツID、認証データ{K_{Pmc1}//C_{mc1}} K_{Pma}、ライセンス購入条件データACを受信し、復号処理部312においてメモリカード110から出力された認証データを公開認証鍵K_{Pma}で復号処理を実行する(ステップS108)。

【0138】配信制御部315は、復号処理部312における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからの公開暗号鍵K_{Pmc1}と証明書C_{mc1}を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS110)。正当な認証データであると判断された場合、配信制御部315は、公開暗号鍵K_{Pmc1}および証明書C_{mc1}を承認し、受理する。そして次の処理(ステップS112)に移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵K_{Pmc1}および証明書C_{mc1}を受理しないで処理を終了する(ステップS170)。

【0139】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであると承認されると、配信制御部315は、次に、メモリカード110のクラス証明書C_{mc1}が禁止クラスリストCRLにリストアップされているかどうかをCRLデータベース306に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する(ステップS170)。

【0140】一方、メモリカード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS112)。

【0141】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ30において、セッションキー発生部316は、配信のためのセッションキーK_{s1}を生成する。セッションキーK_{s1}は、復号処理部312によって得られたメモリカード110に対応する公開暗号鍵K_{Pmc1}によって、暗号化処理部318によって暗号化される(ステップS114)。

【0142】暗号化されたセッションキーK_{s1}は、{K_{s1}} K_{mc1}として、データベースBS1および通信装置350を介して外部に出力される(ステップS116)。

【0143】携帯電話機100が、暗号化されたセッションキー{K_{s1}} K_{mc1}を受信すると(ステップS118)、メモリカード110においては、メモリカードインタフェースを介して、データベースBS3に与えられた受信データを、復号処理部1404が、保持部1402に保持されるメモリカード110固有の秘密復号鍵K_{mc1}により復号処理することにより、セッションキ

ーK_{s1}を復号し抽出する(ステップS120)。

【0144】コントローラ1420は、配信サーバ30で生成されたセッションキーK_{s1}の受理を確認すると、セッションキー発生部1418に対して、メモリカードにおいて配信動作時に生成されるセッションキーK_{s2}の生成を指示する。

【0145】また、配信セッションにおいては、コントローラ1420は、メモリカード110内のメモリ1415に記録されている禁止クラスリストの状態(バージョン)に関連する情報として、リストのバージョンデータCRL_verをメモリ1415から抽出してデータベースBS4に出力する。

【0146】暗号化処理部1406は、切換スイッチ1442の接点Paを介して復号処理部1404より与えられるセッションキーK_{s1}によって、切換スイッチ1444および1446の接点を順次切換えることによって与えられるセッションキーK_{s2}、公開暗号鍵K_{Pm1}および禁止クラスリストのバージョンデータCRL_verを1つのデータ列として暗号化して、{K_{s2}//K_{Pm1}//CRL_ver} K_{s1}をデータベースBS3に出力する(ステップS122)。

【0147】データベースBS3に出力された暗号データ{K_{s2}//K_{Pm1}//CRL_ver} K_{s1}は、データベースBS3からインタフェース1202およびメモリカードインタフェースを介して携帯電話機100に出力され、携帯電話機100から配信サーバ30に送信される(ステップS124)。

【0148】配信サーバ30は、暗号化データ{K_{s2}//K_{Pm1}//CRL_ver} K_{s1}を受信して、復号処理部320においてセッションキーK_{s1}による復号処理を実行し、メモリカード110で生成されたセッションキーK_{s2}、メモリカード110固有の公開暗号鍵K_{Pm1}およびメモリカード110における禁止クラスリストのバージョンデータCRL_verを受理する(ステップS126)。

【0149】禁止クラスリストのバージョン情報CRL_verは、データベースBS1を介して配信制御部315に送られ、配信制御部315は、受理したバージョンデータCRL_verに従って、当該CRL_verのバージョンとCRLデータベース306内の禁止クラスリストデータの現在のバージョンとの間の変化を表わす差分データCRL_datを生成する(ステップS128)。

【0150】さらに、配線制御部315は、ステップS106で取得したコンテンツIDおよびライセンス購入条件データACに従って、ライセンスID、アクセス制限情報AC1および再生回路制御情報AC2を生成する(ステップS130)。さらに、暗号化コンテンツデータを復号するためのライセンスキーK_cを情報データベース304より取得する(ステップS132)。

【0151】図9を参照して、配信制御部315は、生成したライセンス、すなわち、ライセンスキーKcを暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたメモリカード110固有の公開暗号鍵Kpm1によってライセンスキーKc、再生回路制御情報AC2、ライセンスID、コンテンツID、およびアクセス制限情報AC1を暗号化する（ステップS136）。暗号化処理部328は、暗号化処理部326の出力と、配信制御部315がデータベースBS1を介して供給する禁止クラスリストの差分データCRL_dataとを受けて、メモリカード110において生成されたセッションキーKs2によって暗号化する。暗号化処理部328より出力された暗号化データは、データベースBS1および通信装置350を介して携帯電話機100に送信される（ステップS138）。

【0152】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0153】携帯電話機100は、送信された暗号化ライセンス { {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1//CRL_data} Ks2を受信し（ステップS140）、メモリカード110においては、メモリカードインタフェースを介して、データベースBS3に与えられた受信データを復号処理部1412によって復号する。復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてデータベースBS3の受信データを復号しデータベースBS4に出力する（ステップS142）。

【0154】この段階で、データベースBS4には、Km1保持部1421に保持される秘密復号鍵Km1で復号可能な暗号化ライセンス {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1と、CRL_dataとが出力される。コントローラ1420の指示によって、暗号化ライセンス {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1は、メモリ1415に記録される（ステップS144）。一方、暗号化ライセンス {Kc//AC2//ライセンスID//コンテンツID//AC1} Km1は、復号処理部1422において、秘密復号鍵Km1によって復号され、ライセンスのうち、メモリカード110内で参照されるライセンスID、コンテンツIDおよびアクセス制限情報AC1のみが受理される（ステップS146）。

【0155】コントローラ1420は、受理したCRL_dataに基づいて、メモリ1415内の禁止クラスリ

ストデータCRLおよびそのバージョンを更新する（ステップS148）。さらに、メモリ内で参照されるライセンスID、コンテンツIDおよびアクセス制限情報AC1については、ライセンス情報保持部1440に記録される（ステップS150）。

【0156】ステップS150までの処理がメモリ回路で正常に終了した段階で、携帯電話機100から配信サーバ30にコンテンツデータの配信要求がなされる（ステップS152）。

【0157】配信サーバ30は、コンテンツデータの配信要求を受けて、情報データベース304より、暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infを取得して、これらのデータをデータベースBS1および通信装置350を介して出力する（ステップS154）。

【0158】携帯電話機100は、{Data} Kc//Data-infを受信して、暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infを受信する（ステップS156）。暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infはメモリカードインタフェースおよびインタフェース1202を介してメモリカード110のデータベースBS3に伝達される。メモリカード110においては、受信した暗号化コンテンツデータ {Data} Kcおよび付加情報Data-infがそのままメモリ1415に記録される（ステップS158）。

【0159】さらに、メモリカード110から配信サーバ30へは、配信受理の通知が送信され（ステップS160）、配信サーバ30で配信受理を受信すると（ステップS162）、課金データベース302への課金データの格納等を伴って、配信終了の処理が実行され（ステップS164）、全体の処理が終了する（ステップS170）。

【0160】このようにして、携帯電話機100のメモリカード110が正規の機器であること、同時に、クラス証明書Cmc1とともに暗号化して送信できた公開暗号鍵Kmc1が有効であることを確認した上で、それぞれのクラス証明書Cmc1が禁止クラスリスト、すなわち、公開暗号鍵Kmc1による暗号化が破られたクラス証明書リストに記載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0161】図10を参照して、携帯電話機100から得られる情報に基づいてメモリカード110において一対の秘密暗号鍵Kidと公開復号鍵KPidとを生成する動作について説明する。

【0162】鍵生成が開始されると、ユーザは携帯電話機100の操作ボタン部1108から任意のデータを入力する。そうすると、コントローラ1106は、メモリ

カードインタフェースを介して入力されたデータをメモリカード 110 に送付するとともにメモリカード 110 に鍵生成を指示する（ステップ S200）。

【0163】メモリカード 110 のコントローラ 1420 は、インタフェース 1202 およびデータバス BS3 を介して携帯電話機 100 のコントローラ 1106 からの指示を受付け、入力されたデータを鍵生成モジュール 1432 へ送る。そして、鍵生成モジュール 1432 は、入力したデータに基づいて秘密暗号鍵 K i d と、公開復号鍵 K P i d とを生成する（ステップ S201）。公開復号鍵 K P i d は秘密暗号鍵 K i d と非対称であり、秘密暗号鍵 K i d で暗号化されたデータを公開復号鍵 K P i d で復号できることを意味する。

【0164】コントローラ 1420 は、生成された秘密暗号鍵 K i d を鍵生成モジュール 1432 から読出し、K i d 保持部 1433 に記録する（ステップ S202）。また、コントローラ 1420 は、生成された公開復号鍵 K P i d を鍵生成モジュール 1432 から読出し、データバス BS3 およびインタフェース 1202 を介してメモリカードインタフェースへ出力する（ステップ S203）。

【0165】携帯電話機 100 のコントローラ 1106 は、メモリカードインタフェースを介して公開復号鍵 K P i d を受取り、データバス BS2 を介して鍵メモリ 1508 に記録する（ステップ S204）。これで、一対の秘密暗号鍵 K i d と公開復号鍵 K P i d との生成の動作は終了する。

【0166】携帯電話機 100 から入力したデータに基づいて、一対の秘密暗号鍵 K i d と公開復号鍵 K P i d とを生成し、秘密暗号鍵 K i d をメモリカード 110 が保持し、公開復号鍵 K P i d を携帯電話機 100 が保持することにより、メモリカード 110 から携帯電話機 100 へ暗号したデータを送付する際に、携帯電話機 100 という端末装置固有の情報に基づいて生成された鍵を用いることができ、外部からの進入を防止して暗号化されたデータを十分に保護できる。

【0167】図 10 のフローチャートでは、携帯電話機 100 に入力したデータに基づいて一対の秘密暗号鍵 K i d と公開復号鍵 K P i d とを生成したが、本発明ではこれに限らず、携帯電話機 100 のコントローラ 1106 が保持する機器 ID または電話番号に基づいて一対の秘密暗号鍵 K i d と公開復号鍵 K P i d とを生成しても良い。この場合、ステップ S200 において、ユーザは操作ボタン部 1108 から鍵生成を指示するための入力を行なう。そうすると、コントローラ 1106 は、その指示を受付け、保持している機器 ID または電話番号をメモリカードインタフェースを介してメモリカード 110 へ送付する。その後は、図 10 に示すフローチャートに従って一対の秘密暗号鍵 K i d と公開復号鍵 K P i d とが生成され、秘密暗号鍵 K i d がメモリカード 110

の K i d 保持部 1433 で、公開復号鍵 K P i d が携帯電話機 100 の鍵メモリ 1508 で保持される。

【0168】また、一対の秘密暗号鍵 K i d と公開復号鍵 K P i d とは、時刻に基づいて生成されても良い。すなわち、ユーザが配信によってメモリカード 110 に記録した暗号化された音楽データを聞きたいと思ったときの時刻に基づいて一対の秘密暗号鍵 K i d と公開復号鍵 K P i d とが生成される。この場合、ステップ S200 において、ユーザは操作ボタン部 1108 から音楽データの再生指示を入力すると、コントローラ 1106 は、その再生指示を受付けた時刻をタイマー（図示せず）から読取り、メモリカードインタフェースを介してメモリカード 110 へ送付する。その後は、図 10 に示すフローチャートに従って一対の秘密暗号鍵 K i d と公開復号鍵 K P i d とが生成され、秘密暗号鍵 K i d がメモリ 1415 で、公開復号鍵 K P i d が携帯電話機 100 の鍵メモリで保持される。時刻に基づいて一対の秘密暗号鍵 K i d と公開復号鍵 K P i d とが生成されるときは、ユーザが音楽データを聞きたいと思う度ごとに一対の秘密暗号鍵 K i d と公開復号鍵 K P i d とが生成されるため、暗号化されたデータを外部からの進入を防止して十分に保護することができる。

【0169】本発明においては、一対の秘密暗号鍵 K i d と公開復号鍵 K P i d とは端末装置（携帯電話機 100）から得られる情報に基づいて生成される。

【0170】図 11 を参照して、メモリカード 110 に記録された音楽データの再生動作について説明する。再生が開始されると、ユーザは操作ボタン部 1108 から再生指示のための入力を行なう（ステップ S300）。携帯電話機 100 のコントローラ 1106 は、再生指示を受け取ると、認証データ保持部 1500 に保持されている認証データ {K P p 1 / C r t f 1} K P m a をメモリカード 110 へ入力するように指示する（ステップ S301）。メモリカード 110 は、認証データ {K P p 1 / C r t f 1} K P m a を受け取ると、復号処理部 1408 において K P m a 保持部 1414 に保持された公開認証鍵 K P m a を用いて復号し（ステップ S302）、コントローラ 1420 は、復号処理部 1408 における復号処理結果から、認証データ {K P p 1 / C r t f 1} K P m a が正規の認証データであるか否かを判断する認証処理を行なう。さらに、認証データが正規のデータであった場合、コントローラ 1420 は、クラス証明書 C r t f 1 がメモリカード 1415 から読出した禁止クラスリスト C R L に含まれるか否かを判断する（ステップ S303）。すなわち、認証データが正規の認証データであり、かつ、クラス証明書 C r t f 1 が禁止クラスリスト C R L に含まれない場合、認証データ {K P p 1 / C r t f 1} K P m a を承認し、公開暗号鍵 K P p 1 とクラス証明書 C r t f 1 を受理する。

【0171】認証データが正規の認証データでない、あ

るいは、認証データが正規の認証データであってもクラス証明書Crtf1が禁止クラスリストCRLに含まれる場合、認証データ{Kpp1//Crtf1}Kpmaを非承認し、処理を終了する。

【0172】公開暗号鍵Kpp1とクラス証明書Crtf1を受理すると、コントローラ1420は、メモリカードインタフェースを介してメモリカード110へ送付する。そうすると、ステップS304においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報AC1を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数に制限がある場合にはアクセス制限情報AC1のデータを更新し再生可能回数を更新した後に次のステップに進む(ステップS305)。一方、アクセス制限情報AC1によって再生回数が制限されていない場合においては、ステップS305はスキップされ、再生制御情報AC1は更新されることなく処理が次のステップ(ステップS306)に進行される。

【0173】また、ライセンス情報保持部1440内にリクエスト曲の当該コンテンツIDが存在しない場合においても、再生不可の状態にあると判断して、再生動作を終了する。

【0174】ステップS304において、当該再生セッションにおいて再生が可能であると判断された場合には、メモリカード110のセッションキー発生部1418は、セッションキーKs2を発生させる。そして、暗号処理部1406は、発生させたセッションキーKs2を、受理した公開暗号鍵Kpp1を用いて暗号化した{Ks2}Kp1をデータバスBS3、インタフェース1202を介して出力する(ステップS306)。

【0175】携帯電話機100のコントローラ1106の指示に従って、復号処理部1501は、Kp1保持部1502に保持された秘密復号鍵Kp1を用いてメモリカード110から得た{Ks2}Kp1を復号し、得られたセッションキーKs2を受理する(ステップS307)。そして、携帯電話機100のセッションキー発生部1508は、セッションキーKs3を発生させ、発生させたセッションキーKs3を、受理したセッションキーKs2を用いて暗号化した{Ks3}Ks2を、メモリカードインタフェースを介してメモリカード110に与える(ステップS308)。

【0176】メモリカード110のコントローラ1420は、インタフェース1202に入力された{Ks3}Ks2を、データバスBS3を介して復号処理部1412に与える。復号処理部1412は、セッションキー発生部1418によって発生されたセッションキーKs2を用いて{Ks3}Ks2を復号し、セッションキーKs3を受理する(ステップS309)。そしてメモリ1415に記録された再生リクエスト曲のライセンスキーKcや再生情報の復号処理が実行される。具体的には、

コントローラ1420の指示に応じて、メモリ1415からデータバスBS4に読出された暗号化ライセンス{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1を復号処理部1422がメモリカード110固有の秘密復号鍵Km1によって復号し、再生処理に必要なライセンスキーKcと再生回路制御情報AC2がデータバスBS4上に得られる(ステップS310)。

【0177】得られたライセンスキーKcと再生回路制御情報AC2とは、データバスBS3を介して暗号処理部1434に送られる。暗号化処理部1434は、秘密暗号鍵KidによってデータバスBS3から受けたライセンスキーKcと再生回路制御情報AC2を共に暗号化し、{Kc//AC2}KPidをデータバスBS4に出力する(ステップS311)。そして、暗号処理部1406は、データバスBS4上の{Kc//AC2}KPidを、受理したセッションキーKs3を用いて、さらに暗号化し、暗号化データ{{Kc//AC2}KPid}Ks3をデータバスBS3へ出力する(ステップS312)。

【0178】データバスBS3に出力された暗号化データは、インタフェース1202およびメモリカードインタフェースを介して携帯電話機100に送出される。

【0179】携帯電話機100においては、メモリカードインタフェースを介してデータバスBS2に伝達される暗号化データ{Kc//AC2}KPidを復号処理部1510によって復号処理を行ない、暗号化データ{{Kc//AC2}KPid}Ks3を復号処理部1514へ出力する(ステップS313)。復号処理部1514は、鍵メモリ1512に保持されている公開復号鍵KPidによって復号処理を行ない、ライセンスキーKcと再生回路制御情報AC2を受理する(ステップS314)。復号処理部1514は、再生回路制御情報AC2をデータバスBS2に出力する。

【0180】コントローラ1106は、暗号化データ{Kc//AC2}KPidが公開復号鍵KPidを用いて復号されたか否かを判断する(ステップS315)。この判断は、復号されたデータ列Kc//AC2が最後まで意味のあるデータ列を有するか否かによって行われる。すなわち、暗号化データ{Kc//AC2}KPidが鍵メモリ1512に保持された公開復号鍵KPidで復号できないときには、復号処理によって発生する余剰データが意味を持たないデータ列になる。したがって、復号の可否を判断することができる。

【0181】このとき、暗号化データ{Kc//AC2}KPidが復号できないということは、メモリカード110内のKid保持部1433に保持された秘密暗号鍵と携帯電話機100の鍵メモリ1512に保持された公開復号鍵が対応していない、言い換えれば、メモリカード110の所有者と携帯電話機100のユーザとが

異なっていることを意味する。

【0182】その後、再生回路制御情報AC2によって再生の可否が判定される（ステップS316）。

【0183】ステップS316において、再生回路制御情報AC2によって再生不可と判断される場合には、再生動作は終了される。

【0184】暗号化データ {Kc//AC2} KP id が公開復号鍵KP id によって復号でき、かつ、再生回路制御情報によって、携帯電話機100における再生が許されているとき、携帯電話機100のコントローラ1106は、メモリカードインタフェースを介してメモリカード110から暗号化コンテンツデータ {Data} Kcを取得するための指示を出力する。

【0185】そうすると、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ {Data} Kcを読み出して（ステップS317）、データバスBS3およびインタフェース1202を介してメモリカードインタフェースへ出力する（ステップS318）。

【0186】携帯電話機100のコントローラ1106は、メモリカードインタフェースを介して暗号化コンテンツデータ {Data} Kcを取得し、復号処理部1516へ入力する。復号処理部1516は、入力した暗号化コンテンツデータ {Data} Kcを復号処理部1514において復号されたライセンスキーKcによって復号し、符号化コンテンツデータDataを獲得する（ステップS319）。

【0187】復号処理部1516は、符号化コンテンツデータDataを音楽再生部1518へ出力し、音楽再生部1518は、符号化コンテンツデータDataを復調して再生する（ステップS320）。

【0188】DA変換器1519は、音楽再生部1518の出力をデジタル信号からアナログ信号に変換する。そして、再生されたデータは、端子1520、スイッチ1521を介して増幅器1522へ入力され、増幅器1522で増幅されて端子1530からヘッドホン130等へ出力される。これによって暗号化コンテンツデータの再生動作が終了する。

【0189】なお、暗号化コンテンツデータ {Data} Kcの再生は、たとえば、64ビットづつのブロック単位で行われるため、ステップS317～S320が、暗号化コンテンツデータ {Data} Kcが無くなるまで繰返して行われることで音楽が再生される。

【0190】上記の説明においては、配信サーバ30から配信されたライセンスキーKcは、メモリカード110の鍵生成モジュール1432によって生成された秘密暗号鍵K id によって暗号化されずにメモリカード110のメモリ1415に記録されるが（図9のステップS144）、再生に必要なライセンスキーKcと再生回路制御情報AC2とを秘密暗号化K id によって暗号化し

てからメモリ1415に記録しても良い。

【0191】すなわち、図8および図9に示すフローチャートに従って配信動作が進行し、ステップS144までの動作が終了すると、図12に示すように、復号処理部1422は、{Kc//AC2//ライセンスID//コンテンツID//AC1} Km1を、秘密復号鍵Km1によって復号し、ライセンスキーKc、再生回路制御情報AC2、ライセンスID、コンテンツIDおよびアクセス制限情報AC1のみを受理する（ステップS146a）。

【0192】そして、コントローラ1420は、受理したライセンスキーKc、再生回路制御情報AC2と、鍵生成モジュール1432からの秘密暗号鍵K id とを暗号処理部1434へ入力する。暗号処理部1434はライセンスキーKcおよび再生回路制御情報AC2を秘密暗号鍵K id によって暗号化する。コントローラ1420は、暗号化データ {Kc//AC2} KP id をメモリ1415に記録する（ステップS147）。

【0193】その後は、図9のステップS148以降の動作が実行されて配信動作が終了する。

【0194】配信時にコンテンツキーKcを秘密暗号鍵K id によって暗号化してメモリ1415に記録した場合の暗号化コンテンツデータ {Data} Kcの再生動作は、図13に示すように図11のフローチャートのステップS311を省略し、ステップS310をステップS310aに変更したものである。配信時に再生に必要なライセンスキーKcと再生回路制御情報AC2とを秘密暗号鍵K id によって暗号化してメモリ1415に記録しておくことにより再生時に復号処理部1422と暗号処理部1434における処理時間を省略でき、迅速な再生動作が可能である。

【0195】メモリカード110において生成された秘密暗号鍵K id と公開復号鍵KP id とはTRMに記録されるため、外部からの進入を排除して一対の秘密暗号鍵K id と公開復号鍵KP id とを管理できるとともに、一対の秘密暗号鍵K id と公開復号鍵KP id とを用いて暗号化コンテンツデータを十分に保護しながら再生できる。

【0196】上記においては、暗号化コンテンツデータと、暗号化コンテンツデータを復号するライセンスキーとは携帯電話網を用いてメモリカード110に配信されると説明したが、それ以外の方法によって配信されても良い。

【0197】図14を参照して、コンピュータ140を用いた暗号化コンテンツデータの配信について説明する。携帯電話機100にはメモリカード110が着脱可能であり、音楽を再生するためのヘッドホン130が接続されている。そして、携帯電話機100は、通信ケーブル145を介してコンピュータ140と接続されて

【0198】コンピュータ140は、ハードディスク141と、コントローラ142と、外部インタフェース143とを備える。そして、ハードディスク141はデータバスBS5を介してコントローラ142と接続され、コントローラ142はライセンス保護モジュール143を含む。

【0199】ハードディスク141は、インターネット配信によってコンピュータ140に配信された暗号化コンテンツデータをデータバスBS5を介して記憶する。コントローラ142は、携帯電話機100のユーザから通信ケーブル145および外部インタフェース143を介して暗号化コンテンツデータの送信要求があると、ハードディスク141から暗号化コンテンツデータを読み出し、外部インタフェース143を介して外部へ出力する。

【0200】外部インタフェース143は、携帯電話機100から通信ケーブル145を介してコンピュータ140に入力された信号をコントローラ142に入力するとともに、コントローラ142からの信号を外部へ出力する。

【0201】ライセンス保護モジュール144は、図5に示すデータ処理部310と同じ構成を有し、携帯電話機100に装着されたメモリカード110に暗号化コンテンツデータを送信するために、上述したように携帯電話機100およびメモリカード110と公開暗号鍵、セッションキー等のやり取りを行ないながら、暗号化コンテンツデータを保護してメモリカード110へ送信するものである。

【0202】インターネット配信によって配信サーバからコンピュータ140に暗号化コンテンツデータが配信され、コンピュータ140のハードディスク141にデータバスBS5を介して暗号化コンテンツデータが記憶されている。

【0203】携帯電話機100のユーザが操作ボタン部1108から送信要求を入力すると、通信ケーブル145および外部インタフェース143を介して送信要求がコントローラ142に入力される。コントローラ142は、送信要求を受付けると、要求された暗号化コンテンツデータをデータバスBS5を介してハードディスク141から読み出し、ライセンス保護モジュール144に入力する。

【0204】ライセンス保護モジュール144は、上述したようにメモリカード110と通信ケーブル145を介して公開暗号鍵、セッションキー等のやり取りを行ない、暗号化コンテンツデータをメモリカード110へ送信する。

【0205】送信後、携帯電話機100のユーザは、上述したのと同じ方法によって暗号化コンテンツデータを再生する。

【0206】また、コンピュータ140は、インターネ

ット配信によって暗号化コンテンツデータを受信しなくても良く、暗号化コンテンツデータが記録されたCD-ROMをコンピュータ140に接続されたCD-ROMドライブ（図示せず）に装着し、そのCD-ROMから暗号化コンテンツデータを読み出してメモリカード110へ送信しても良い。また、CD-ROMに記録された暗号化コンテンツデータを、一旦、ハードディスク141に記憶しておいても良い。

【0207】なお、図14において、コンピュータ140は暗号化コンテンツデータを復号するためのコンテンツキーを携帯電話機100へ送信しない。コンテンツキーは、別途、携帯電話網等を介して携帯電話機100へ配信され、その時、著作権料が課金される。

【0208】さらに、コンピュータ140は、CDリッピングによって暗号化コンテンツデータとライセンスを生成しても良い。リッピングとは、音楽CDから取得した音楽データを、音楽再生モジュールで再生できるように変換することを言う。まず、取得した音楽データに対してライセンスを生成する。次いで、取得した音楽データを音楽再生部1518にて再生可能なコンテンツデータに変換した後、生成したライセンスに含まれるコンテンツキーにて復号可能な暗号化を行なうもので、リッピングによって得られた暗号化コンテンツデータの生成されたライセンスには、複製ができないように管理される。したがって、音楽CDからの1次複製であるCDリッピングは、コンテンツの暗号化と、その復号鍵であるコンテンツキーを含むライセンスが複製できない構成を取ることによって著作権を保護した適法な行為である。

【0209】CDを用いた場合、音楽CDから取得して生成した暗号化コンテンツデータとライセンスは、一旦、ハードディスク141に記録してからメモリカード110へ送信しても良いし、ハードディスク141に送信せずに、直接、メモリカード110へ送信しても良い。

【0210】暗号化コンテンツデータは、図15に示すようにメモリカード110を、直接、コンピュータ140に装着してメモリカード110に暗号化コンテンツデータを記録しても良い。この場合、コンピュータ140のコントローラ142は、ライセンス保護モジュール144によって、直接、メモリカード110に暗号化コンテンツデータを記録する。

【0211】図15においても、コンピュータ140は、図14に示す場合と同じ方法により暗号化コンテンツデータを取得する。

【0212】なお、上記説明においては、秘密暗号鍵K_{id}と公開復号鍵K_{Pid}とは、携帯電話機100のID、および携帯電話機100の電話番号等の携帯電話機100から入力された情報に基づいて非対称に生成されると説明したが、本発明においては、これに限らず、共通鍵方式のように、携帯電話機100のID、および携

携帯電話機100の電話番号等の携帯電話機100から入力された情報に基づいて対称に生成されてもよい。

【0213】実施の形態として暗号化されたコンテンツデータと、その復号鍵であるライセンスキーを含むライセンスを記録するメモリカードにおけるライセンスの記録あるいは出力における暗号を用いたライセンスの受け渡しによるコンテンツ保護について説明したが、ライセンスを用いないでコンテンツデータの記録あるいは出力において暗号を用いて保護するようにしても同様の効果が得られる。

【0214】さらに、音楽データや画像データなどのコンテンツデータのみでなくデータ全般に対しても適用することが可能である。

【0215】また、コントローラを備えたメモリカードに限らず、コントローラを備えたハードディスク等の他の記録媒体であっても適用可能である。

【0216】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 データ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。。

【図5】 ライセンスサーバの構成を示す概略ブロック図である。

【図6】 実施の形態による携帯電話機の構成を示すブロック図である。

【図7】 実施の形態によるメモリカードの構成を示すブロック図である。

【図8】 図1に示すデータ配信システムにおける配信動作を説明するための第1のフローチャートである。

【図9】 図1に示すデータ配信システムにおける配信動作を説明するための第2のフローチャートである。

【図10】 携帯電話機から入力した情報に基づく一対

の秘密暗号鍵と公開復号鍵との生成を説明するためのフローチャートである。

【図11】 実施の形態における携帯電話機における再生動作を説明するためのフローチャートである。

【図12】 図1に示すデータ配信システムにおける配信動作を説明するための他の第2のフローチャートである。

【図13】 実施の形態における携帯電話機における再生動作を説明するための他のフローチャートである。

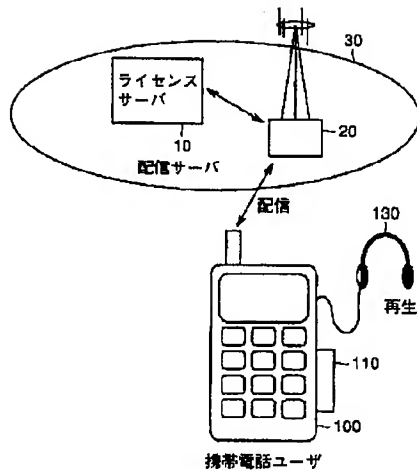
10 【図14】 他のデータ配信システムを概念的に説明する概略図である。

【図15】 さらに他のデータ配信システムを概念的に説明する概略図である。

【符号の説明】

10 ライセンスサーバ、20 配信キャリア、30 配信サーバ、100 携帯電話機、110 メモリカード、130 ヘッドホン、140 コンピュータ、141 ハードディスク、142, 1106, 1420 コントローラ、143, 1107 外部インタフェース、144, 1450 ライセンス保護モジュール、145 通信ケーブル、302 課金データベース、304 情報データベース、306 CRLデータベース、310 データ処理部、312, 320, 1404, 1408, 1412, 1422, 1504, 1510, 1514, 1516 復号処理部、315 配信制御部、316, 1418, 1508セッションキー発生部、318, 326, 328, 1406, 1410, 1434, 1506 暗号処理部、350 通信装置、1102 アンテナ、1104 送受信部、1108 操作ボタン部、1110 ディスプレイ、1112 音声再生部、1113, 1519 DA変換器、1114, 1520, 1530端子、1200 メモリカードインタフェース、1202 インタフェース、1402 Kmc1保持部、1414 KPma保持部、1415 メモリ、1416 KPm1保持部、1421 Km1保持部、1440 ライセンス情報保持部、1442, 1444, 1446 切換スイッチ、1400, 1500認証データ保持部、1432 鍵生成モジュール、1433 Kid保持部、1502 Kp1保持部、1512 鍵メモリ、1518 音楽再生部、1521スイッチ、1522 増幅器、1550 音楽再生モジュール。

【図 1】



【図 2】

名称	属性	保持/発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ
Kc	ライセンスキー		暗号化コンテンツデータの復号鍵
{Data}Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータ この形式で配信サーバより配布。
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード (コンテンツIDを含めて識別することも可)
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数、機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話機)における制御情報 (例：再生可否)

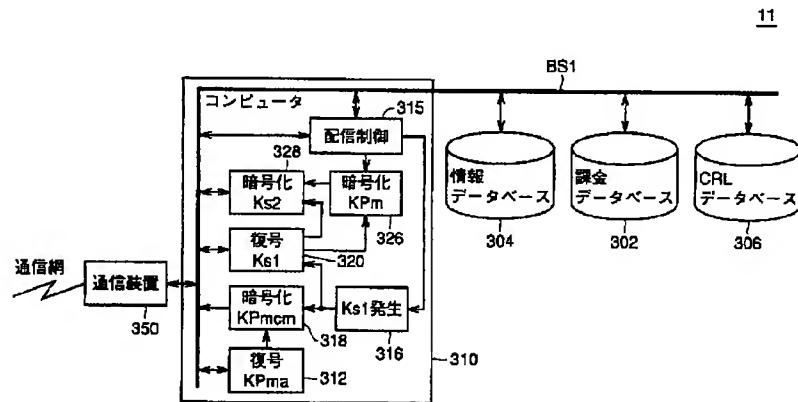
【図 3】

名称	属性	保持/発生箇所	機能・特徴
CRL	禁止クラスリスト関連情報	配信サーバ	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報 (差分データ形式)
CRL_ver		メモ리카ード	禁止クラスリストのバージョン情報
KPpn	公開暗号鍵 (非対称鍵)	携帯電話機	Kpnにて復号可能。 {KPpn/Crtfn}KPmaの形式で出荷時に記録 *携帯電話機の種類nごとに異なる。
KPmcm	公開暗号鍵 (非対称鍵)	メモ리카ード	Kmcmにて復号可能。 {KPmcm/Cmcm}KPmaの形式で出荷時に記録 *メモ리카ードの種類mごとに異なる。
Kpn	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の復号鍵 *携帯電話機の種類nごとに異なる。
Kmcm	秘密復号鍵	メモ리카ード	メモ리카ード固有の復号鍵 *メモ리카ードの種類mごとに異なる。
Crtfn	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。 認証データ{KPpn/Crtfn}KPmaの形式で出荷時に記録 *携帯電話機のクラスnごとに異なる。
Cmcm		メモ리카ード	メモ리카ードのクラス証明書。認証機能を有する。 認証データ{KPmcm/Cmcm}KPmaの形式で出荷時に記録 *メモ리카ードのクラスmごとに異なる。

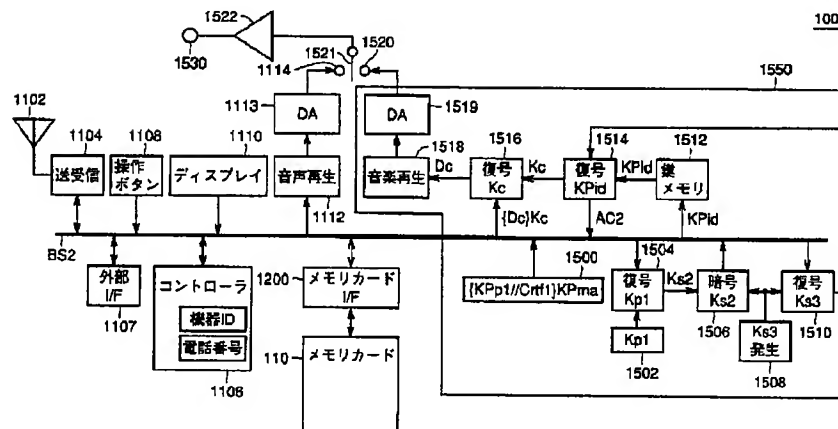
【図 4】

名称	属性	保持／発生箇所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／再生セッション毎に発生
Ks3		携帯電話機	再生セッション毎に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵 Kpmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵 (非対称鍵)	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開認証鍵	配信サーバ	配信システム全体で共通。
KPid	公開復号鍵	携帯電話機 メモリカード	携帯電話機から得られる情報に基づいて 生成され、再生セッションに用いられる。
Kid	秘密暗号鍵	メモリカード	携帯電話機から得られる情報に基づいて 生成され、再生セッションに用いられる。

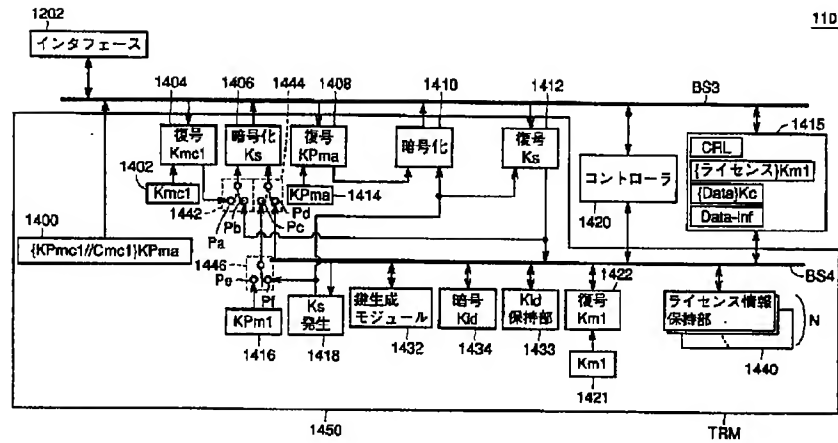
【図 5】



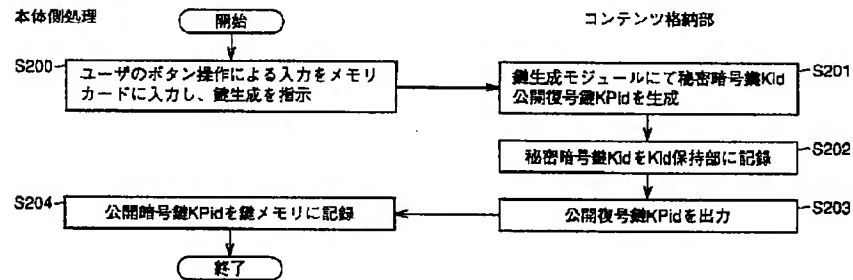
【图 6】



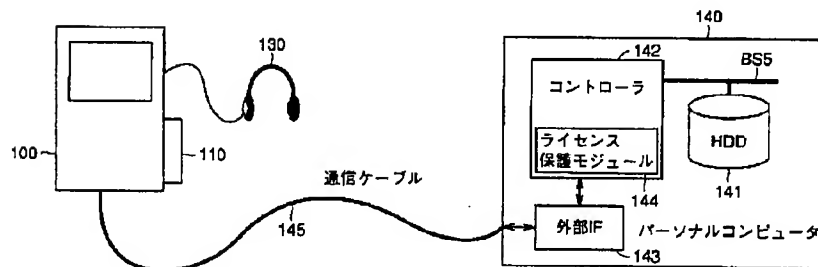
【図7】



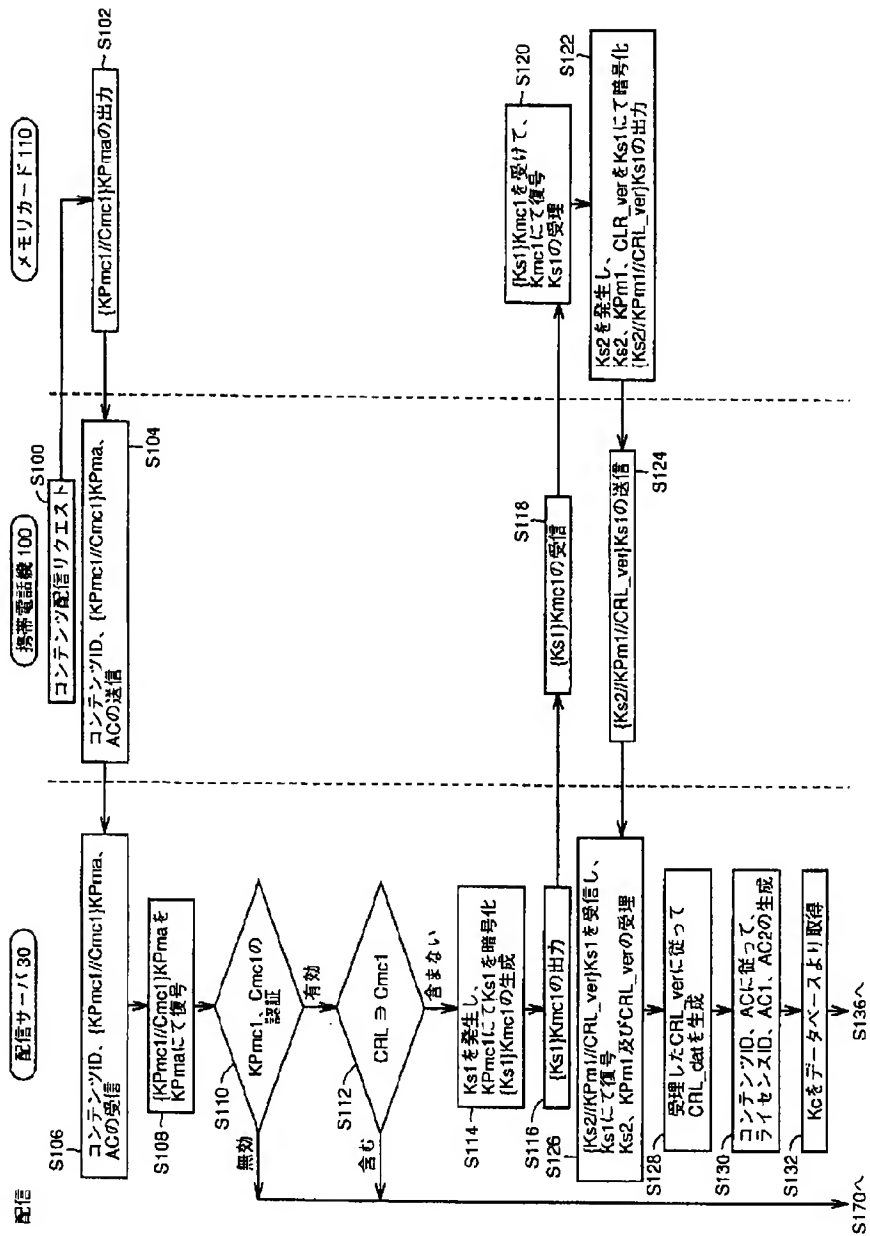
【図10】



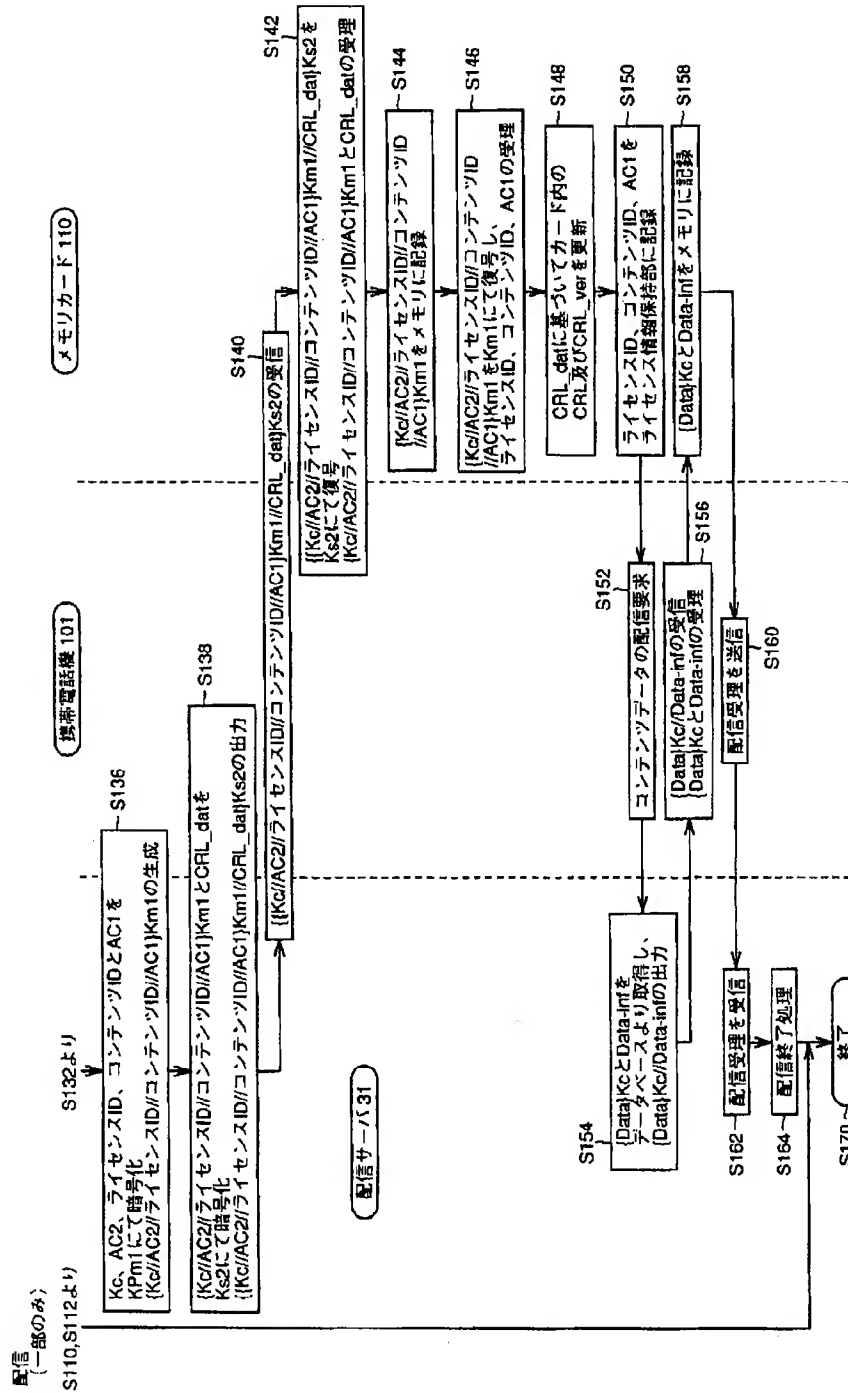
【図14】



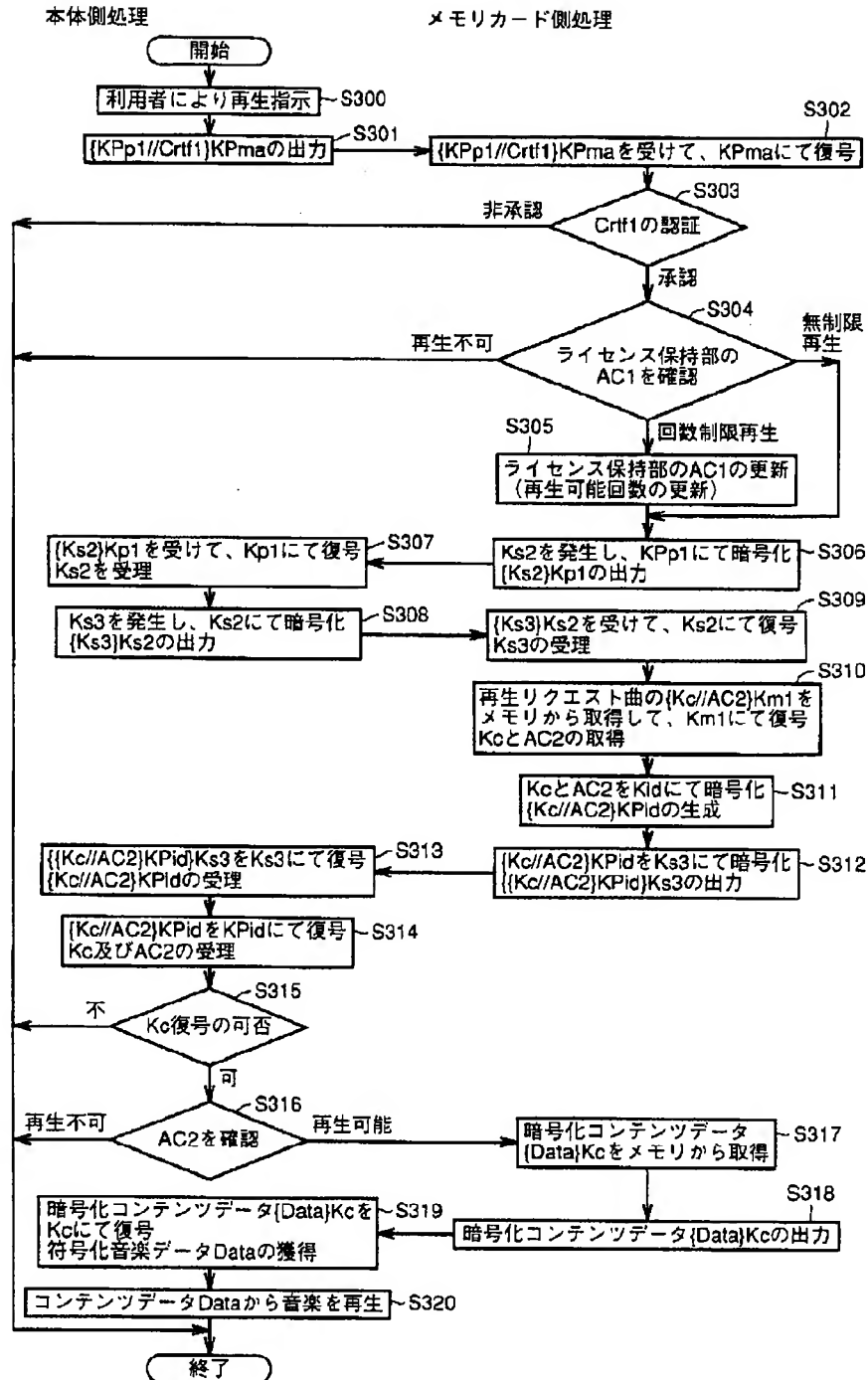
【図8】



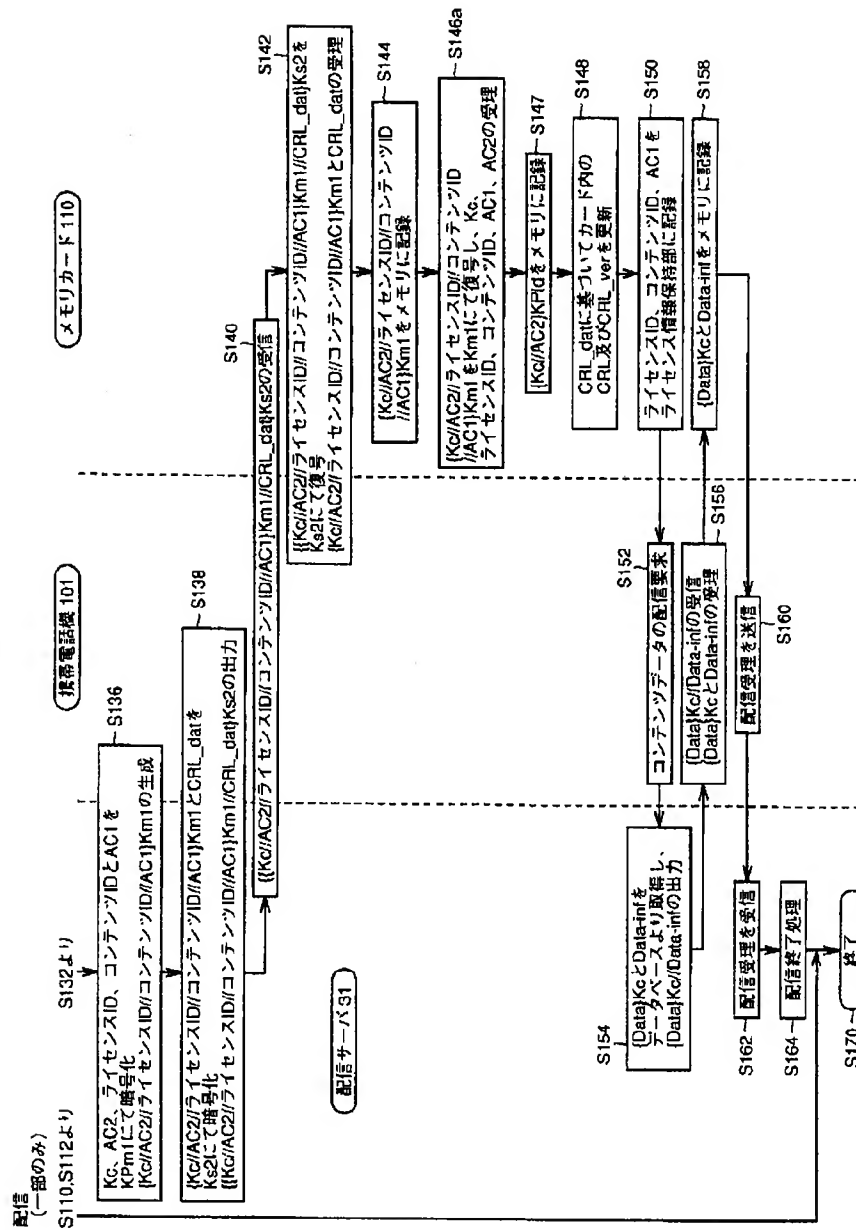
【図9】



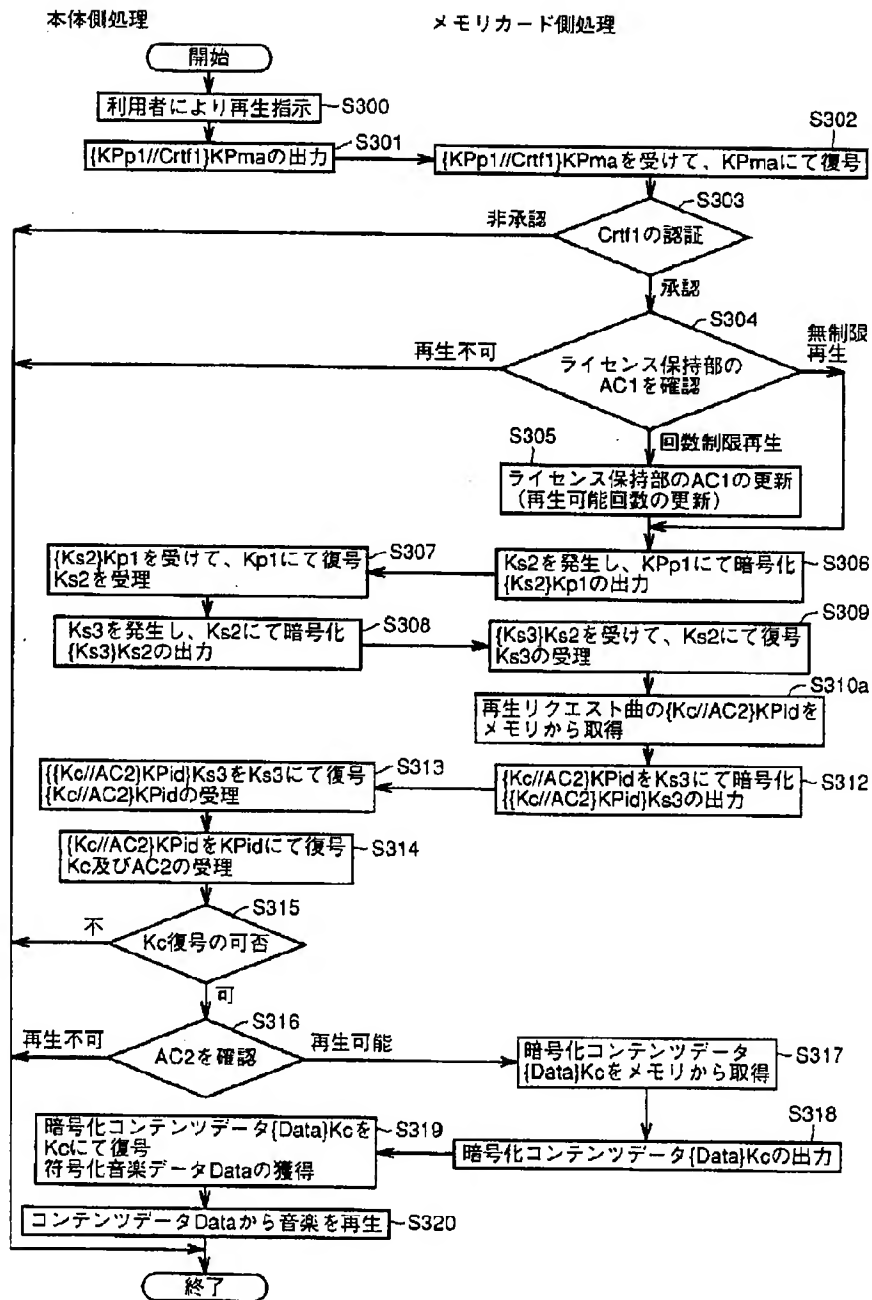
【図11】



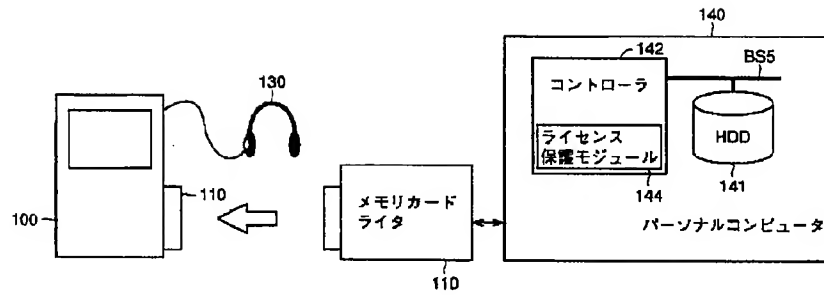
【図12】



【図13】



【図 15】



フロントページの続き

(51) Int. Cl.⁷

識別記号

F I

ターマコード* (参考)

H 0 4 N 7/167

Z

(72) 発明者 堀 吉宏

大阪府守口市京阪本通 2 丁目 5 番 5 号 三
洋電機株式会社内

F ターム (参考) 5B085 AE02 AE12 AE13 AE23 AE29

5C064 CB08

5J104 AA01 AA07 AA16 EA04 KA05

KA10 MA02 NA02 PA02 PA07

PA14

5K067 AA30 BB04 DD17 DD52 DD54

FF04 FF07 FF40 HH23 HH24

HH36 KK15